WEB APPLICATION FIREWALL

FortiWeb-VM Install Guide

VERSION 5.6

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

September 23, 2016

FortiWeb 5.6 Install Guide

1st Edition

TABLE OF CONTENTS

Overview of FortiWeb-VM

Welcome, and thank you for selecting Fortinet products to protect your network.

FortiWeb-VM is a virtual appliance version of FortiWeb. FortiWeb-VM models are suitable for medium and large enterprises, as well as service providers.

Benefits

FortiWeb is designed specifically to protect web servers.

FortiWeb web application firewalls (WAF) provide specialized application layer threat detection and protection for many HTTP or HTTPS services, including:

- Apache Tomcat
- nginx
- Microsoft IIS
- JBoss
- IBM Lotus Domino
- Microsoft SharePoint
- Microsoft Outlook Web App (OWA)
- RPC and ActiveSync for Microsoft Exchange Server
- Joomla
- WordPress

FortiWeb's integrated web vulnerability scanner can drastically reduces challenges associated with protecting regulated and confidential data by detecting your exposure to the latest threats, especially the OWASP Top 10.

In addition, FortiWeb's XML firewall and denial-of-service (DoS) attack-prevention protect your Internet-facing web-based applications from attack and data theft. Using advanced techniques to provide bidirectional protection against sophisticated threats like SQL injection and cross-site scripting (XSS), FortiWeb helps you prevent identity theft, financial fraud, and corporate espionage. FortiWeb delivers the technology you need to monitor and enforce government regulations, industry best practices, and internal security policies, including firewalling and patching requirements from PCI DSS.

FortiWeb's application-aware firewalling and load balancing engine can:

- Secure HTTP applications that are often gateways into valuable databases
- Prevent and reverse defacement
- Improve application stability
- Monitor servers for downtime & connection load
- Reduces response times
- Accelerate SSL/TLS *
- Accelerate compression/decompression
- Rewrite content on the fly

* On VM models, acceleration is due to offloading the cryptography burden from the back-end server. On hardware models with ASIC chips, cryptography is also hardware-accelerated.

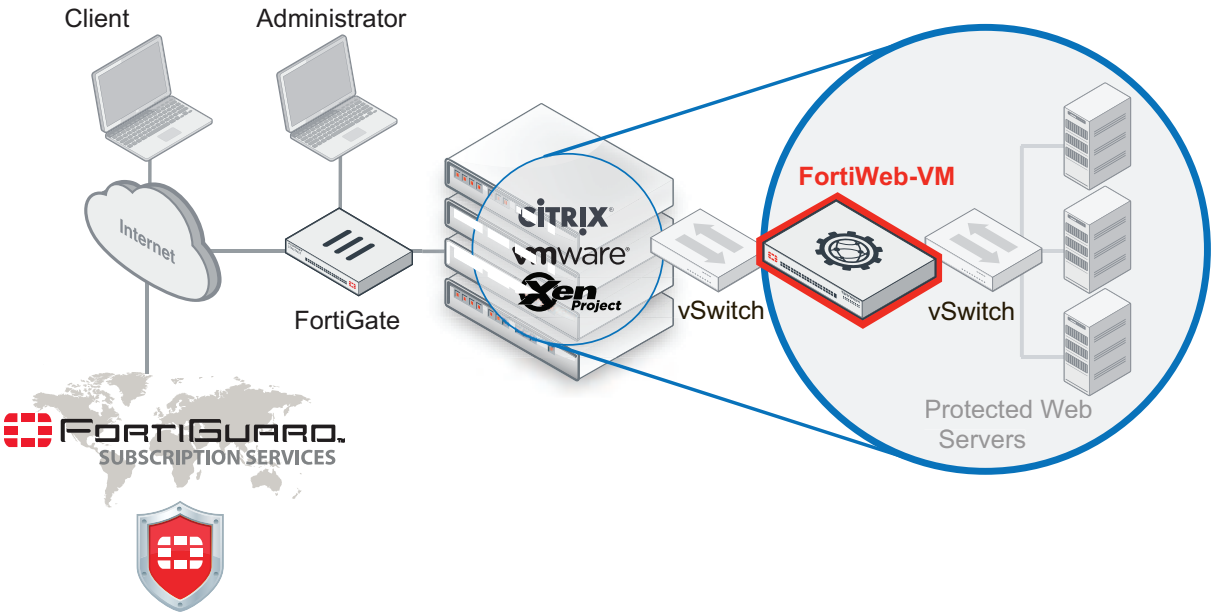
FortiWeb significantly reduces deployment costs by consolidating WAF, hardware acceleration, load balancing, and vulnerability scanning into a single device with no per-user pricing. Those features drastically reduce the time required to protect your regulated, Internet-facing data and eases the challenges associated with policy enforcement and regulatory compliance.

Architecture

FortiWeb-VM is deployed in the following environments:

- virtual machine, such as VMware vSphere (see illustration)
- Amazon Web Services (AWS) EC2, as an Amazon Machine Image (AMI)
- OpenStack cloud computing platform

FortiWeb-VM network topology



FortiWeb can be deployed in a one-arm topology, but is more commonly positioned inline to intercept all incoming clients' connections and redistribute them to your servers. FortiWeb has TCP- and HTTP-specific firewalling capability. Because it is not designed to provide security to non-HTTP applications, it should be deployed behind a firewall such as FortiGate that focuses on security for other protocols that can be forwarded to your back-end servers, such as FTP and SSH.

Once the virtual appliance is deployed, you can configure FortiWeb-VM via its web UI and CLI, from a web browser and terminal emulator on your management computer.

FortiWeb-VM requires Internet connectivity.

- DNS lookup — UDP 53
- FortiGuard licensing — TCP 443

Licensing

Hypervisor and AWS BYOL deployments use FortiWeb-VM licenses that determine the size of the virtual appliance. The registration number you use to obtain the license is also required to dowload software (for hypervisor deployments) and register for FortiGuard services and technical support.

(Licensing for FortiWeb Manager is different. See the *FortiWeb Manager Handbook*.)

On-demand/hourly FortiWeb-VM from AWS includes a fully-licensed instance of FortiWeb-VM, all FortiGuard services, and technical support. No separate license file is required.

FortiWeb-VM licenses are available at the sizing levels described in the table.

FortiWeb-VM resource limitations

	License/model			
	VM01	**VM02**	**VM04**	**VM08**
Virtual CPUs (vCPUs)	1	2	4	8

Maximum IP sessions and policies varies by license, but also by available vRAM, just as it does for hardware models. For details, see maximum configuration values in the *FortiWeb Administration Guide*.

When you place an order for FortiWeb-VM, Fortinet emails a registration number to the recipient address you supplied on the order form. To register your appliance with Technical Support and to obtain a license file, enter that registration number on the Fortinet Technical Support web site at the following location:

https://support.fortinet.com/

The license file is required to permanently activate FortiWeb-VM. For details, see Downloading the FortiWeb-VM license & registering with Technical Support on page 17.

FortiWeb-VM needs to periodically re-validate its license by contacting either Fortinet's FortiGuard Distribution Network (FDN) via an Internet connection or a FortiManager.

If FortiWeb-VM cannot contact FDN or FortiManager for 24 hours, it locks access to the web UI and CLI. In some cases, the web UI displays a message such as:

```
License has been uploaded. Please wait for authentication with
registration servers.
```

For information on restoring access or configuring license validation using FortiManager, see Uploading the license on page 149.

Evaluation limitations

Hypervisor FortiWeb-VM deployments include a free 15-day trial license that includes all features **except** :

- High availability (HA)
- FortiGuard updates
- Technical support

You do not need to manually upload the trial license. It is built-in. The trial period begins the first time you start FortiWeb-VM.

Once the trial expires, most functionality is disabled. You need to purchase a license to continue using FortiWeb-VM.

AWS BYOL FortiWeb-VM deployments do not include the free trial license. Instead, you can evaulate FortiWeb using the on-demand/hourly version from AWS.

FortiWeb Manager virtual machine

FortiWeb Manager is a specialized VM model that you use to provision, configure, and update FortiWeb appliances (either VM or hardware-based). You use the same steps to install a FortiWeb-VM and the FortiWeb Manager virtual machine, but FortiWeb Manager performs management tasks only and does not include FortiWeb itself.

FortiWeb Manager's evaluation license has different limitations and the steps for uploading a license are different from FortiWeb-VM.

For more information, see the *FortiWeb Manager Administration Guide*.

About this document

Scope

This document provides the following information:

- How to deploy a FortiWeb virtual appliance disk image onto a virtualization server, AWS EC2 environment, or OpenStack cloud computing platform
- How to configure any required virtual hardware settings. For hypervisor deployments, it assumes you have already successfully installed a virtualization server on the physical machine or the required EC2 enviroment.

This document does **not** cover initial configuration of the virtual appliance, nor ongoing use and maintenance.

After deploying the virtual appliance, for information on initial appliance configuration, see the *FortiWeb Administration Guide* or *FortiWeb Manager Administration Guide*.

This document is intended for administrators, not end users. If you have a user account on a computer that accesses web sites through a FortiWeb appliance, please contact your system administrator.

Conventions

This document uses the conventions described below.

IP addresses

To avoid IP conflicts that would occur if you used examples in this document with public IP addresses that belong to a real organization, the IP addresses used in this document are fictional. They belong to the private IP address ranges defined by these RFCs.

RFC 1918: Address Allocation for Private Internets

http://ietf.org/rfc/rfc1918.txt?number-1918

RFC 5737: IPv4 Address Blocks Reserved for Documentation

http://tools.ietf.org/html/rfc5737

RFC 3849: IPv6 Address Prefix Reserved for Documentation

http://tools.ietf.org/html/rfc3849

For example, even though a real network's Internet-facing IP address would be routable on the public Internet, in this document's examples, the IP address would be shown as a non-Internet-routable IP such as 10.0.0.1, 192.168.0.1, or 172.16.0.1.

Cautions, notes, & tips

This document uses the following guidance and styles for notes, tips and cautions.

Warns you about procedures or feature behaviors that could have unexpected or undesirable results including loss of data or damage to equipment.

Highlights important, possibly unexpected but non-destructive, details about a feature's behavior.

Presents best practices, troubleshooting, performance tips, or alternative methods.

Typographical conventions

This document uses the following typefaces to indicate items such as code or button names.

Typographical conventions in this document

Convention	Example
Button, menu, text box, field, or check box label	From **Minimum log level**, select **Notification**.

CLI input	`config system dns`
	`  set primary <address_ipv4>`
	`end`

CLI output	`FortiWeb# diagnose hardware logdisk info`
	`disk number: 1`
	`disk[0] size: 31.46GB`
	`raid level: no raid exists`
	`partition number: 1`
	`mount status: read-write`

Emphasis	HTTP connections are **not** secure and can be intercepted by a third party.
File content	<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4></BODY></HTML>
Hyperlink	https://support.fortinet.com

Convention	Example
Keyboard entry	Type the IP address or domain name of an NTP server or pool, such as `pool.ntp.org`.
Navigation	Go to **System > Status > Status**.
Publication	For details, see the *FortiWeb Administration Guide*.

Command syntax conventions

The command line interface (CLI) requires that you use valid syntax, and conform to expected input constraints. It will reject invalid commands.

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

Command syntax notation

Convention	Description

Square brackets [ ]	A non-required (optional) word or words. For example:
	`[verbose {1 | 2 | 3}]`
	indicates that you may either omit or type both the `verbose` word and its accompanying option, such as:
	`verbose 3`

Curly braces { }	A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [ ].
Options delimited by vertical bars |	Mutually exclusive options. For example: `{enable | disable}` indicates that you must enter either `enable` or `disable`, but must not enter both.

Options delimited by spaces	Non-mutually exclusive options. For example:
	`{http https ping snmp ssh telnet}`
	indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as:
	`ping https ssh`

Convention	Description
	Note: To change the options, you must re-type the entire list. For example, to add `snmp` to the previous example, you would type: `ping https snmp ssh` If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.
Angle brackets < >	A word constrained by data type. To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (_) and suffix that indicates the valid data type. For example: `<retries_int>` indicates that you should enter a number of retries, such as `5`. Data types include: • `<xxx_name>` — A name referring to another part of the configuration, such as `policy_A`. • `<xxx_index>` — An index number referring to another part of the configuration, such as `0` for the first static route.
	• `<xxx_pattern>` — A regular expression or word with wild cards that matches possible variations, such as `*@example.com` to match all e-mail addresses ending in `@example.com`. • `<xxx_fqdn>` — A fully qualified domain name (FQDN), such as `mail.example.com`. • `<xxx_email>` — An email address, such as `admin@mail.example.com`. • `<xxx_url>` — A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as `http://www.fortinet.com/`. • `<xxx_ipv4>` — An IPv4 address, such as `192.168.1.99`.
	• `<xxx_v4mask>` — A dotted decimal IPv4 netmask, such as `255.255.255.0`. • `<xxx_ipv4mask>` — A dotted decimal IPv4 address and netmask separated by a space, such as `192.168.1.99 255.255.255.0`. • `<xxx_ipv4/mask>` — A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as such as `192.168.1.99/24`. • `<xxx_ipv6>` — A colon(`:`)-delimited hexadecimal IPv6 address, such as `3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234`. • `<xxx_v6mask>` — An IPv6 netmask, such as `/96`. • `<xxx_ipv6mask>` — An IPv6 address and netmask separated by a space.

Convention	Description
	• `<xxx_str>` — A string of characters that is **not** another data type, such as `P@ssw0rd`. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. See the *FortiWeb CLI Reference*. • `<xxx_int>` — An integer number that is **not** another data type, such as `15` for the number of minutes.

What's new

The list below contains features new to or changed **in the VM version of the firmware only** since FortiWeb 5.4.

FortiWeb 5.6

- **KVM ttyS0 console support** — You can now configure a FortiWeb-VM instance you deploy on KVM with the console "/dev/ttyS0" in addition to the console "/dev/console".

  In the information on deploying FortiWeb-VM on KVM, see Import the FortiWeb-VM virtual machine on page 120.

FortiWeb 5.5 Patch 4

- **Deploy FortiWeb-VM on OpenStack** — You can now use the KVM version of the FortiWeb-VM software to deploy a virtual appliance on the OpenStack cloud computing platform using Cloud Init.

FortiWeb 5.5 Patch 2 - FortiWeb 5.5 Patch 3

- No changes specific to the VM version of the firmware.

FortiWeb 5.5 Patch 1

- **Support for VMware vSphere HA** — vSphere High Availability (HA) allows you to pool virtual machines and the hosts they reside on into a cluster. In the event of a failure, the HA feature restarts the virtual machines on a failed host on alternate hosts. This alternative to FortiWeb HA requires no HA configuration on the FortiWeb.

  See Configuring vSphere HA and Fault Tolerance on page 48.

- **Support for VMware Tools** — VMware Tools is now included when you deploy FortiWeb-VM on vSphere. VM Tools allows FortiWeb-VM to work with native vSphere functionality, such as vSphere HA and Fault Tolerance and guest system shutdown and restart.

FortiWeb 5.5

- No changes specific to the VM version of the firmware.

FortiWeb 5.4

- **FortiWeb Manager virtual machine** — The new FortiWeb central manager solution is a standalone virtual instance running on VMware vSphere ESXi. It replaces the existing solution. See FortiWeb Manager virtual machine on page 8.
- **Support for KVM (Kernel-based Virtual Machine)** — You can now deploy FortiWeb-VM on Linux using KVM. See Deploying FortiWeb-VM on KVM on page 120.
- **Default memory allocation** — By default, FortiWeb-VM is installed with 4 G of vRAM on VMware vSphere ESXi, Citrix XenServer, and open source Xen Project.
- **Support for 1 to 10 ports** — FortiWeb-VM can now support any number of network interfaces from 1 and 10.

System requirements

FortiWeb-VM installation requires one of the following environments:

- Virtual machine (VM) environment software (a hardware abstraction layer (HAL) that is sometimes called a hypervisor) on your server. FortiWeb-VM is a virtual appliance that runs inside this environment.

  FortiWeb-VM supports the following hypervisor versions:

  - VMware vSphere Hypervisor ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0
  - Citrix XenServer 6.2/6.5
  - open source Xen Project (Hypervisor) 4.0.1, 4.1, 4.2, 4.4
  - Microsoft Hyper-V (version 6.2 or higher, running on Windows 8 or higher, or Windows Server 2012)
  - KVM (Linux kernel 2.6, 3.0, or 3.1)
  - OpenStack Liberty 12.0.0

For best performance in hypervisor deployments, install FortiWeb-VM on a “bare metal” (type 1) hypervisor, such as VMware ESXi or Xen. Hypervisors that are installed as applications on top of a general purpose operating system (Windows, Mac OS X or Linux) host have fewer computing resources available due to the host OS’s own overhead.

  For hypervisor installation instructions, see the documentation for your VM environment.

  For hypervisor deployments, hardware-assisted virtualization (Intel VT or AMD-V) must be enabled in the BIOS. You must also have the VM environment client, such as VMware vSphere Client, installed on a management computer. (A management computer is a desktop or a laptop that you use to deploy and manage your virtual machines.)

- An Amazon Web Services’ Elastic Compute Cloud (Amazon EC2) account with an Amazon Virtual Private Cloud (Amazon VPC).

  AWS deployments of FortiWeb-VM support reverse proxy operation mode only.

  The following types of AWS deployments are available:

  - BYOL (Bring Your Own License)
  - On-demand/hourly
- OpenStack cloud computing platform

  OpenStack deployment does not support true transparent proxy or transparent inspection operation modes.

Downloading the FortiWeb-VM license & registering with Technical Support

For Hypervisor and AWS BYOL deployments, when you purchase FortiWeb-VM from your reseller, you receive an email that contains a registration number. You use this number to download the software and your purchased license, and also to register your purchase for technical support.

Many Fortinet customer services such as firmware updates, technical support, and FortiGuard services require product registration.

For on-demand/hourly FortiWeb-VM from Amazon Web Services (AWS), no separate license is required. Your purchase includes a fully-licensed instance of FortiWeb-VM, all FortiGuard services, and technical support.

For more information, see the Fortinet Knowledge Base article Registration Frequently Asked Questions.

To register & download your FortiWeb-VM license

1. On your management computer, start a web browser.
2. Log in to the Fortinet Technical Support web site:

   https://support.fortinet.com/
3. In the **Asset Management** quadrant of the page, click **Register/Renew**.
4. Provide the registration number that was emailed to you when you purchased the software. Registration numbers are a hyphenated mixture of 25 numbers and characters in groups of 5. For example:

   `12C45-AB3DE-678G0-F9HIJ-123B5`

   A registration form is displayed.
5. Complete the form to register your ownership of FortiWeb-VM with Technical Support.

   After you complete the form, a registration acknowledgement page is displayed.
6. Click the **License File Download** link.

   Your browser downloads the `.lic` file that was purchased for that registration number.
7. Do one of the following:
   - If you are installing the virtual appliance on your own hypervisor instance, download the FortiWeb software using the steps in Downloading the FortiWeb-VM software.
   - If you are using Amazon Web Services with EC2, use the EC2 console to download a special firmware build configured as an Amazon Machine Image (AMI). See Deploying FortiWeb-VM on AWS EC2.

Downloading the FortiWeb-VM software

To download your FortiWeb-VM software

1. On the main page of the Fortinet Technical Support web site, under **Download**, click **Firmware Images**.
2. Click the FortiWeb link and navigate to the version that you want to download.
3. Download the appropriate `.zip` file.

   You use this file for **new virtual appliance (VM)** installations. It contains a deployable virtual machine package. (`.out` image files are for upgrades of existing installations only, and cannot be used for a new installation.)

Files for FortiWeb-VM have a `FWB_VM` file name prefix. Other prefixes indicate that the file is for hardware versions of FortiWeb such as FortiWeb 4000D. These hardware versions are not used with FortiWeb-VM.

If you have a library of virtual machine images stored on a CIFS or NFS share, download and unzip the folder there instead of on your management computer. When deploying the VM, you can also use a CIFS or NFS network share as the storage repository instead of a vDisk stored locally, on the hypervisor's disk.

4. Extract the `.zip` compressed archive's contents to a folder.
5. Continue by deploying the virtual appliance package using the appropriate deployment instructions in this guide.

   For example, see Deploying FortiWeb-VM on VMware vSphere on page 22.

Deploying FortiWeb-VM on AWS EC2

There are two ways to deploy FortiWeb-VM on Amazon Web Services' Elastic Compute Cloud (Amazon EC2):

- **Bring Your Own License (BYOL)** — Requires a FortiWeb-VM license (see Downloading the FortiWeb-VM license & registering with Technical Support on page 17).
- **On-demand** — Provides a fully-licensed instance of FortiWeb-VM, all FortiGuard services, and technical support on an hourly basis.

Both methods require an existing Amazon EC2 account and Amazon Virtual Private Cloud (Amazon VPC).

You can deploy the FortiWeb-VM for AWS using either the AWS Marketplace **1-Click Launch** option or directly from the EC2 Console.

For FortiWeb-VM on Amazon Web Services (AWS), the default password for the `admin` administrator is the AWS instance ID.

To deploy FortiWeb-VM for AWS from AWS Marketplace

1. Log in to AWS and ensure that you have a VPC (Virtual Private Cloud).

   You add VPCs using the AWS Management Console.
2. Go to the AWS Marketplace home page (aws.amazon.com/marketplace) and log in with your credentials.
3. To navigate to the appropriate FortiWeb-VM product page, either go to the **Security** category or search for "fortinet".
4. Navigate to the product page for FortiWeb-VM or FortiWeb-VM (BYOL).
5. Click **Continue**.
6. Select the appropriate region and EC2 instance type for your deployment.
7. Under **Security Group**, ensure that **Create new based on seller settings** is selected.

   The only open port that is required for the initial FortiWeb-VM configuration is 443. This port allows you to connect to the web UI via HTTP. However, these default security group settings configure the instance for all potential FortiWeb communication.
8. Use the instructions provided under **Key Pair** to create a new key pair.

   Creating a key pair allows you to access the command-line interface via SSH.
9. Click **Accept Terms & Launch with 1-Click**.
10. Click **Manage in AWS Console** to access the virtual appliance instance and the public DNS address. You use this address to connect to FortiWeb and configure the appliance.
11. Use the public DNS address to do one of the following:
    - Connect to the web UI.

      For example, if the public DNS address is `ec2-54-234-142-136.compute-1.amazonaws.com`, you

connect to the web UI using the following URL:

`https://ec2-54-234-142-136.compute-1.amazonaws.com/`

To log in to the virtual appliance, for **Name**, enter `admin`. The default `admin` password is the AWS instance ID.

- Connect to the command-line interface (CLI) using an SSH connection. See To connect to the CLI using an SSH connection on page 20.

12. Do one of the following:

- For FortiWeb-VM (BYOL), continue with the instructions in Uploading the license on page 149.
- For on-demand FortiWeb-VM, configure the FortiWeb-VM software using the *FortiWeb Administration Guide*.

If you change the size of the FortiWeb-VM virtual hard disk after deployment, immediately run the following command:

`execute formatlogdisk`

You can run the command using the **CLI Console** widget on the dashboard or via an SSH connection (see To connect to the CLI using an SSH connection on page 20).

For information about how to use the CLI, see the *FortiWeb CLI Reference*.

The `formatlogdisk` command clears logs from the virtual hard disk, reformats the disk, and clears the `admin` account password that is used with FortiWeb-VM AWS deployments.

To log in to the FortiWeb-VM web UI or CLI using `admin` after running `formatlogdisk`, leave the password blank.

AWS can only auto-assign a public IP address to a single, new network interface with the device index eth0. If you add additional network interfaces to your FortiWeb-VM instance, the Auto-assign Public IP list is not available and you cannot access the instance via the public IP address AWS assigned earlier.

If you need to add additional network interfaces, first manually associate an elastic IP address with the primary network interface.

To connect to the CLI using an SSH connection

These instructions connect to FortiWeb-VM using PuTTY terminal emulation software.

1. On your management computer, start PuTTY.

2. To ensure that your configuration does not use environment variables that can interfere with the connection, in the **Category** tree, expand **Connection**, and then click **Data.** Remove any environment variables.
3. Click **Session**, and for **Host Name (or IP Address)**, enter the public DNS address of the FortiWeb-VM instance.

   For example, `ec2-54-234-142-136.compute-1.amazonaws.com`.
4. In Port, type `22`.
5. For **Connection type**, select **SSH**.
6. Select **Open**.

   The SSH client connects to the FortiWeb appliance.

   The SSH client may display a warning if this is the first time you are connecting to the FortiWeb appliance and its SSH key is not yet recognized by your SSH client, or if you have previously connected to the FortiWeb appliance but it used a different IP address or SSH key.
7. Click **Yes** to verify the fingerprint and accept the FortiWeb appliance's SSH key. You cannot log in until you accept the key.

   The CLI displays a login prompt.
8. Type `admin` and press Enter.
9. For password, enter the AWS instance ID, which is the default password.

If 3 incorrect login or password attempts occur in a row, FortiWeb temporarily blacklists your IP address from the GUI and CLI. This action protects the appliance from brute force login attacks. Wait 1 minute, and then attempt the login again.

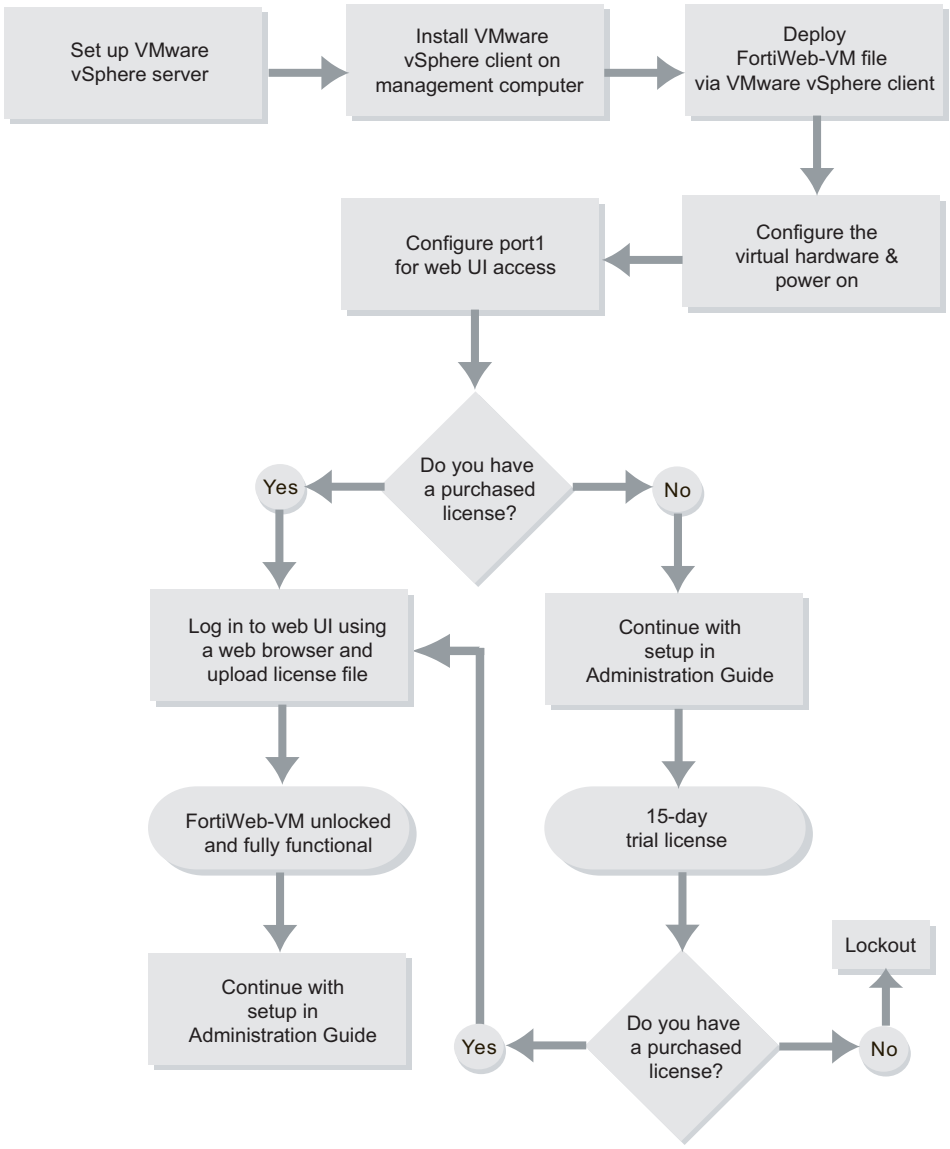
The CLI displays a prompt, such as:

FortiWeb `#`

Deploying FortiWeb-VM on VMware vSphere

The diagram below overviews the process for installing FortiWeb-VM on VMware vSphere, which is described in the subsequent text.

Basic steps for installing FortiWeb-VM (VMware)



Deploying the OVF file

Before you can configureFortiWeb-VM, you must first use VMware vSphere Client to deploy the FortiWeb-VM OVF package.

To deploy the virtual appliance

1. On your management computer, start VMware vSphere Client.

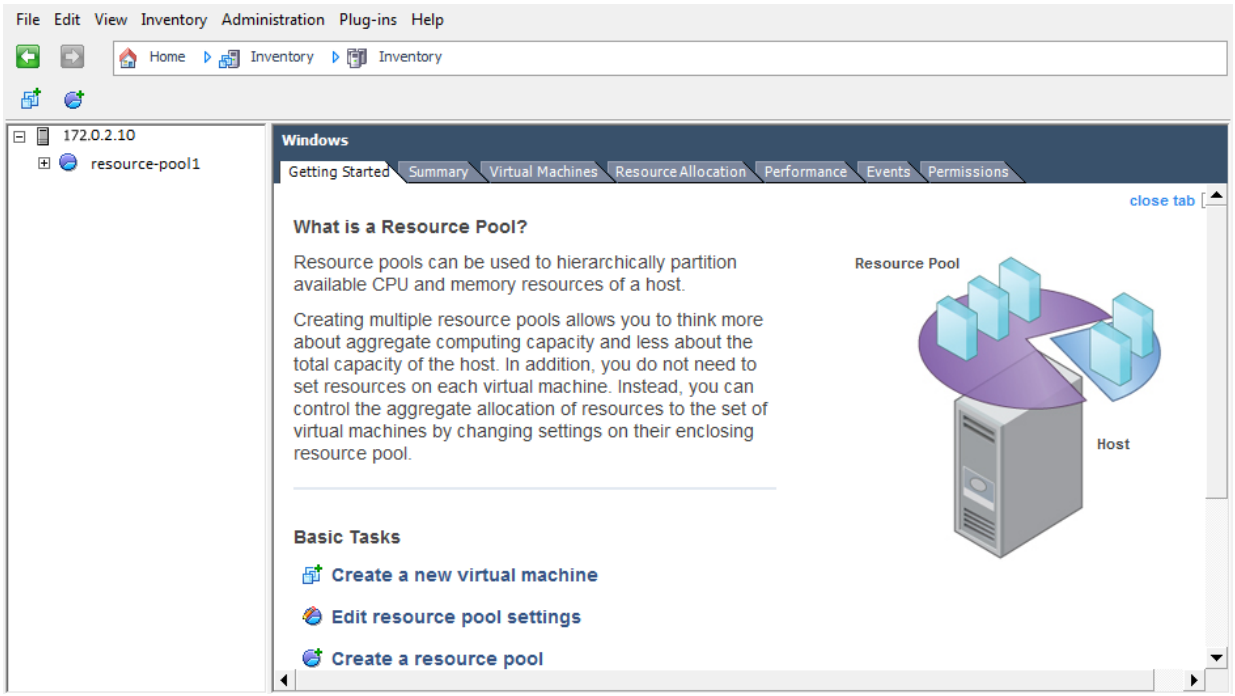
In **IP address / Name**, type the IP address or FQDN of the VMware vSphere server.

In **User name**, type the name of your account on that server.

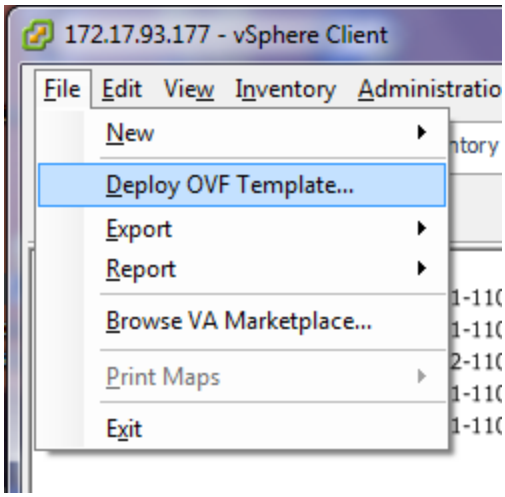
In **Password**, type the password for your account on that server.

Click *Login*.

When you successfully log in, the vSphere Client window appears.

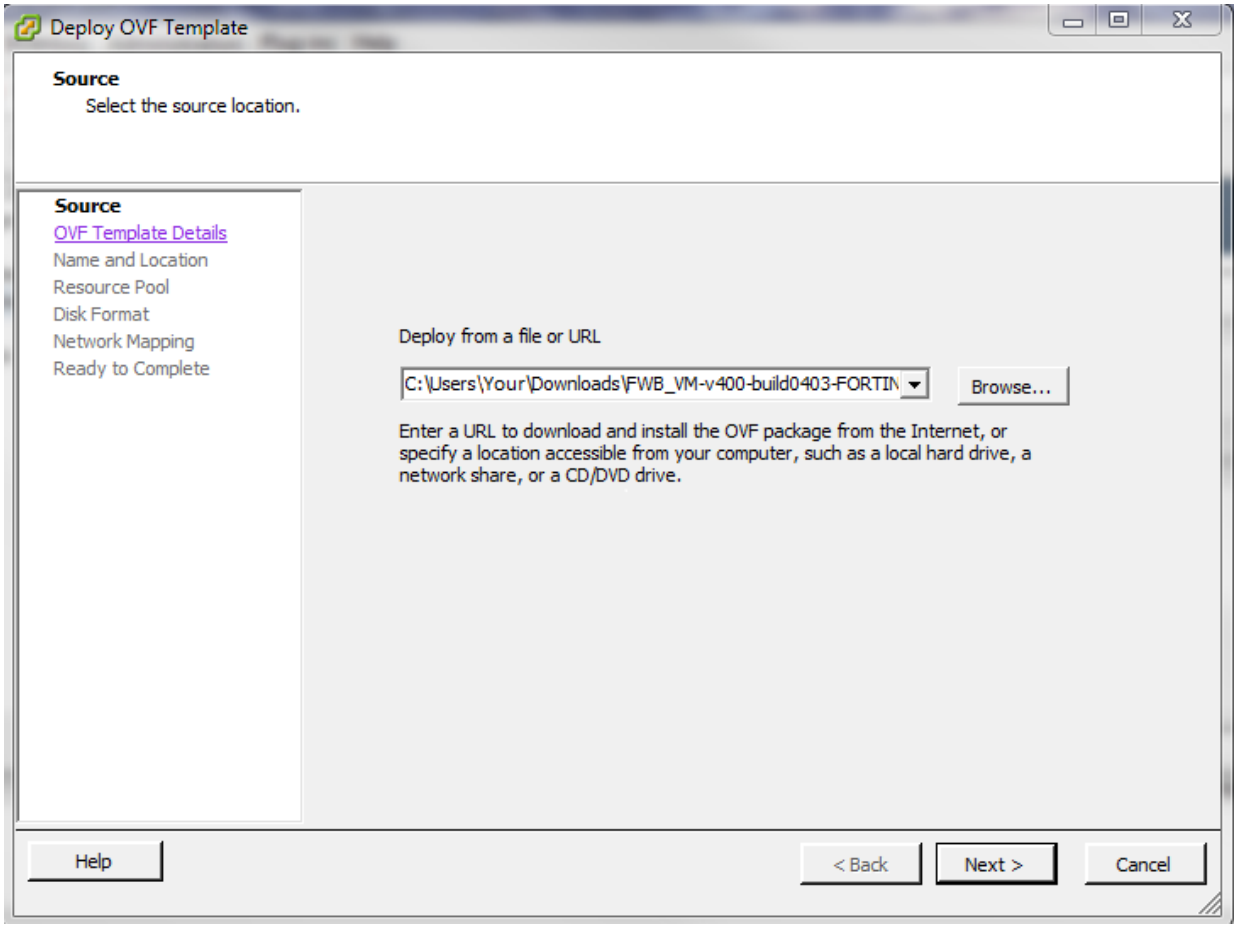


2. Go to **File > Deploy OVF Template**.



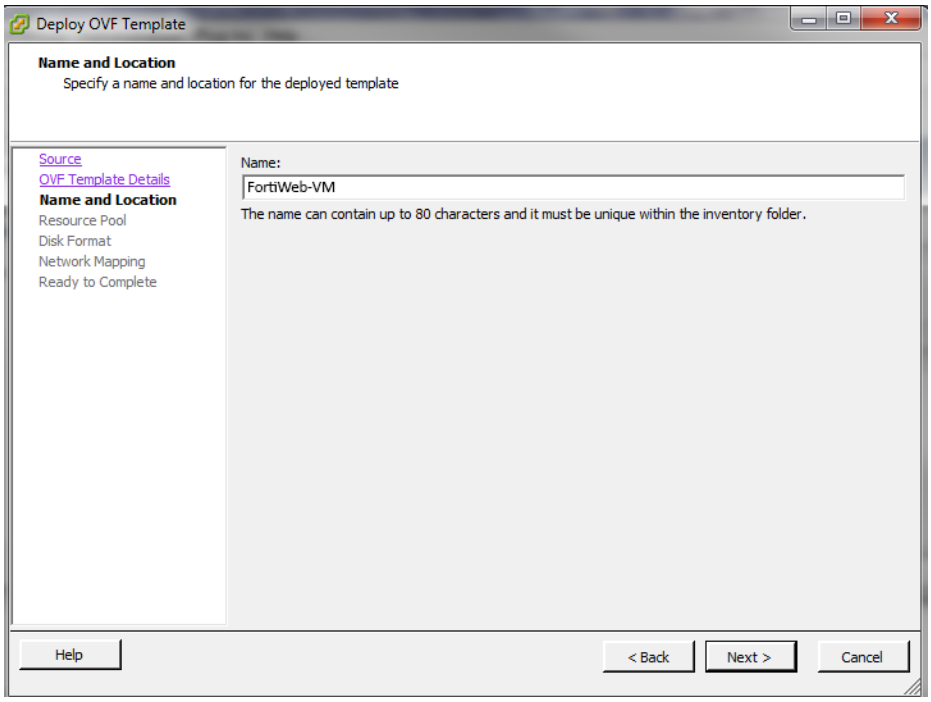
A deployment wizard window appears.

3. In the **Deploy OVF Template** window, click **Browse**, then locate the FortiWeb-VM OVF file.

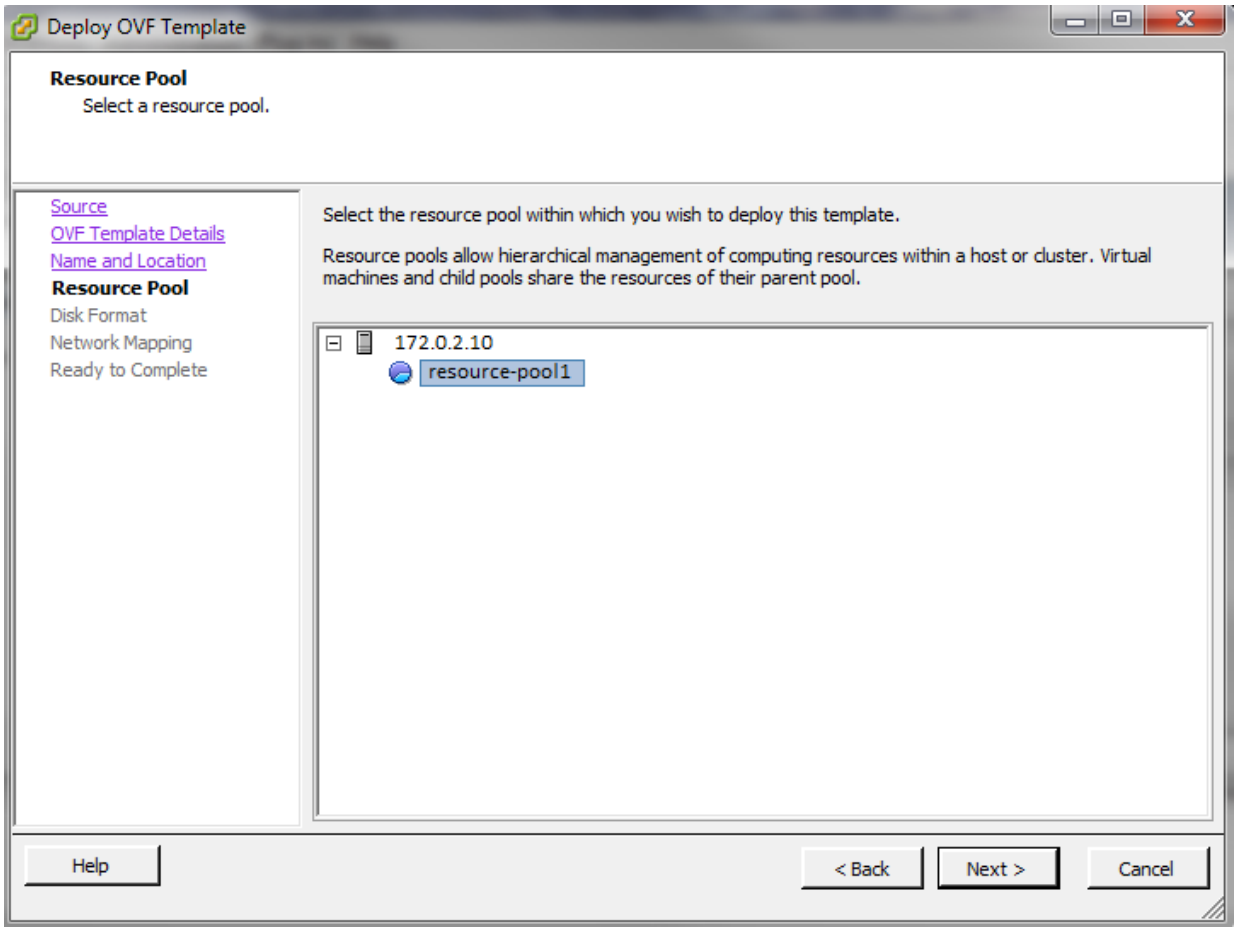


4. Click **Next** twice.

5. In **Name**, type a unique descriptive name for this instance of FortiWeb-VM as it will appear in vSphere Client's inventory, such as `FortiWeb-VM`. If you will deploy multiple instances of this file, consider a naming scheme that will make each VM's purpose or IP address easy to remember. (This name will not be used as the host name, nor will it appear within the FortiWeb-VM web UI.)

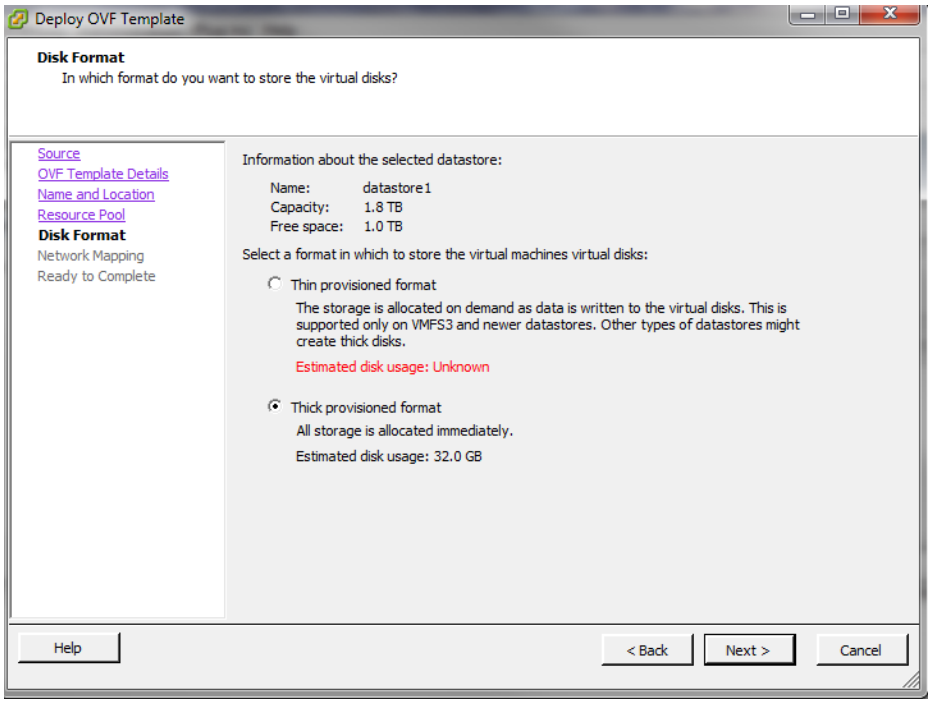


6. Click **Next**.
7. In the resource pool tree, select a virtual machine.



8. Click **Next**.
9. For the storage repository, select either:
   - **Thin provisioned format** — Allocate more disk space on demand, if the storage repository uses a VMFS3 or newer file system.

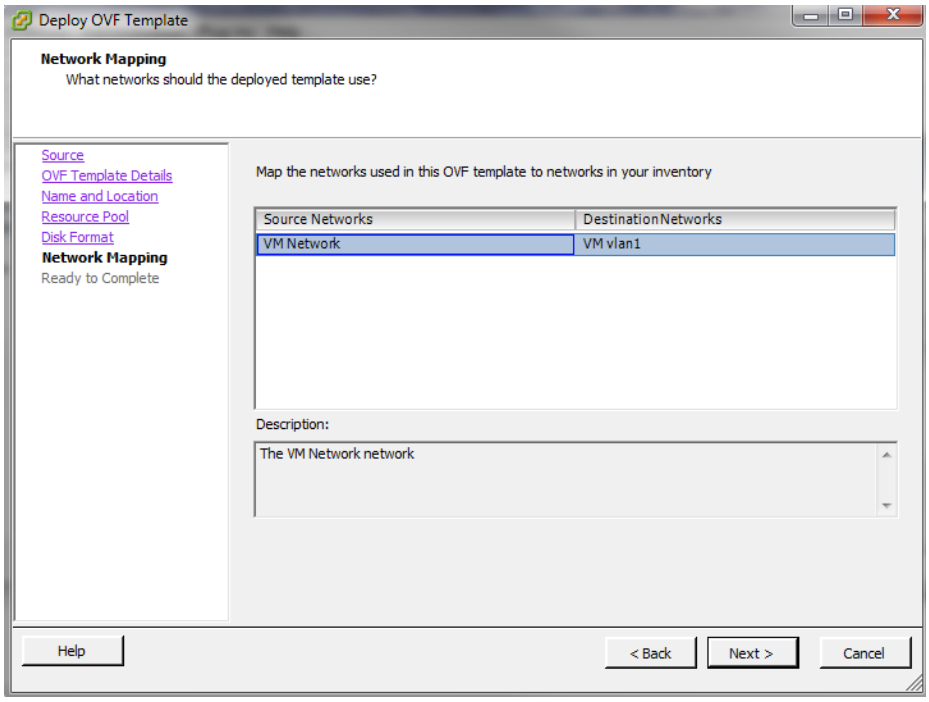
- **Thick provisioned format** — Immediately allocate disk space (specifically 32 GB) for the storage repository



Regardless of your choice here, you must later either allocate or make available at least 40 GB of disk space. 32 GB is only the default minimum value, and is not recommended..

10. Click **Next**.

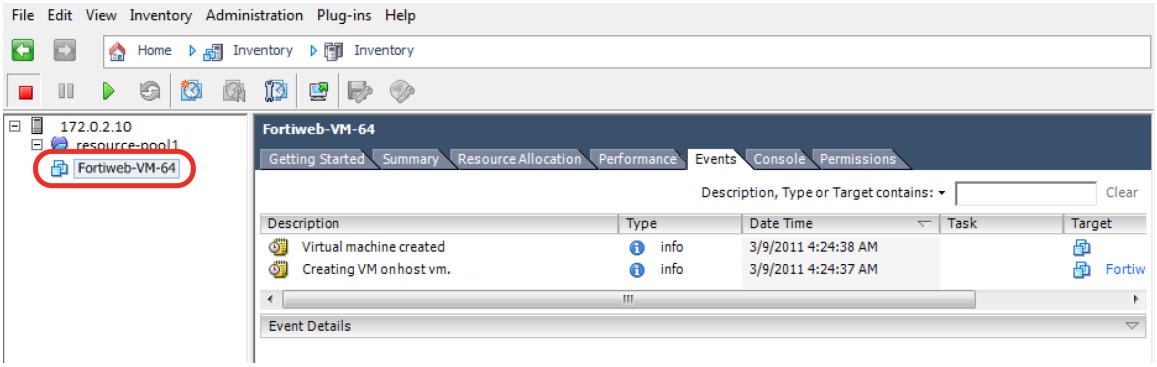
11. If the hypervisor has more than one possible network mapping for its vSwitch, click to select the row for the network mapping that FortiWeb-VM should use.



12. Click **Next**.
13. Click **Finish**.

    The wizard closes. The client connects to the VM environment and deploys the OVF to it. Time required depends on your computer's hardware speed and resource load, and also on the file size and speed of the network connection, but might take several minutes to complete.

    The vSphere Client window reappears. The navigation pane's list of virtual machines on the left now should include your new instance of FortiWeb-VM.



Continue with Configuring the virtual appliance's virtual hardware settings on page 29.

Do **not** power on the virtual appliance **until** you:

- Resize the virtual disk (VMDK) (see Resizing the virtual disk (vDisk) on page 29)
- Set the number of vCPUs (see Configuring the number of virtual CPUs (vCPUs) on page 32)
- Set the vRAM on the virtual appliance (Configuring the virtual RAM (vRAM) limit on page 34)
- Map the virtual network adapter(s) (Mapping the virtual NICs (vNICs) to physical NICs on page 36).

These settings cannot be configured inside FortiWeb-VM, and must be configured in the VM environment. **Some settings cannot be easily reconfigured after you power on the virtual appliance.**

Configuring the virtual appliance's virtual hardware settings

After installing FortiWeb-VM, log in to VMware vSphere on the server and configure the virtual appliance's hardware settings to suit the size of your deployment. For sizing guidelines, contact your reseller or Fortinet Technical Support.

For information on the limits of configurable values for FortiWeb-VM, see the *FortiWeb Administration Guide*.

Resizing the virtual disk (vDisk)

If you configure the virtual appliance's storage repository to be internal (i.e. local, on its own vDisk), resize the vDisk **before** powering on.

This step is not applicable if the virtual appliance will use external network file system (such as NFS) datastores.

The FortiWeb-VM package that you downloaded includes pre-sized VMDK (Virtual Machine Disk Format) files. However, they are only 32 GB, which is not large enough for most deployments. **Resize the vDisk before powering on the virtual machine.**

Before doing so, make sure that you understand the effects of your vDisk settings.

For example, if you have an 800 GB data store which has been formatted with 1 MB block size, you cannot size a single vDisk greater than 256 GB on your FortiWeb-VM.

Consider also that, depending on the size of your organization's network, you might require more or less storage for your auto-learning data, anti-defacement backups, scan results, and reports.

For more information on vDisk sizing, see:

http://communities.vmware.com/docs/DOC-11920

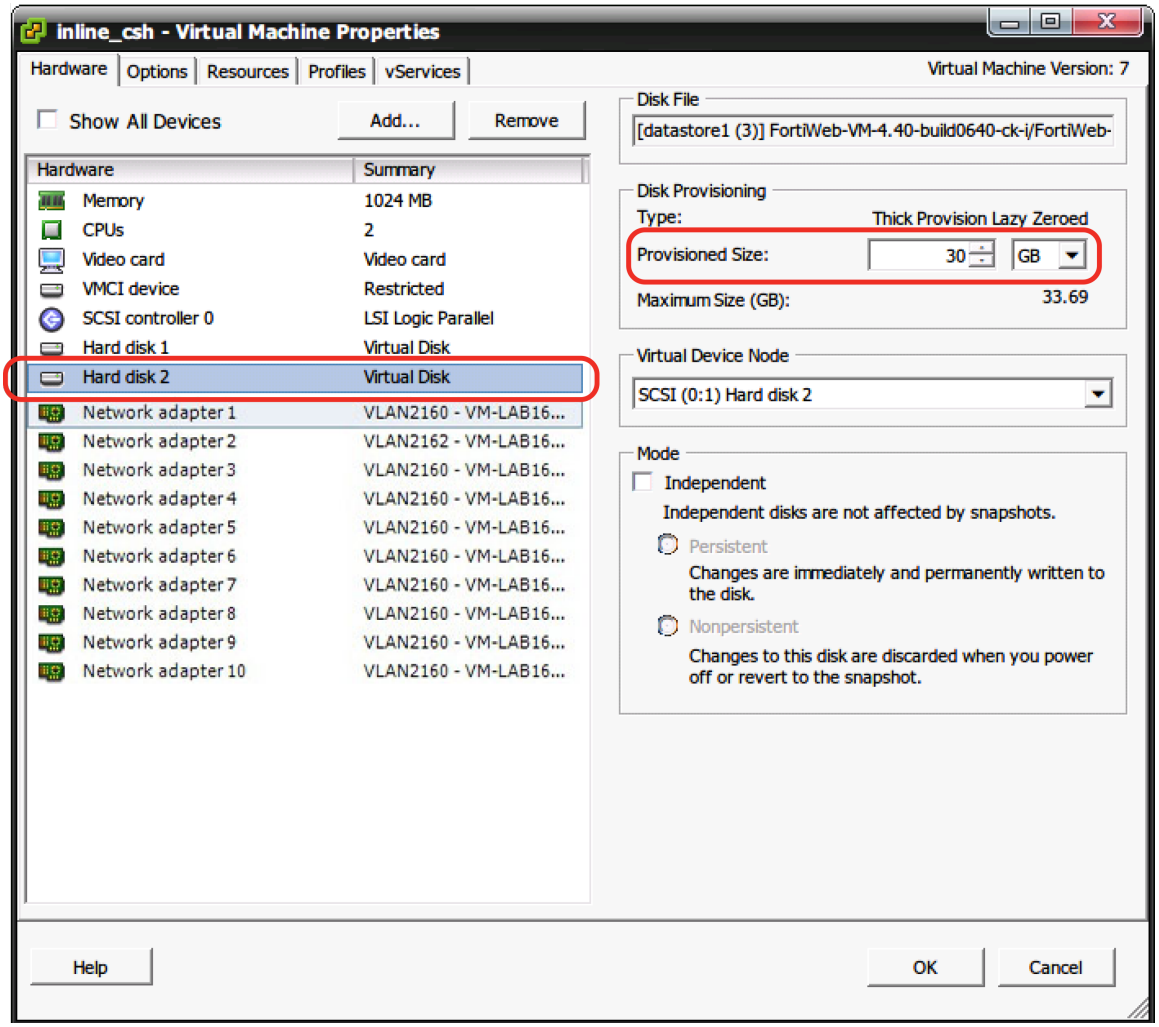
To resize the vDisk

If you are resizing the disk for an existing deployment of FortiWeb-VM, back up the logs and other non-configuration data **before** beginning this procedure. **Formatting the disk will delete all data on that disk.** For backup instructions, see the *FortiWeb Administration Guide*.

While resizing the vDisk, the FortiWeb-VM must be powered off.

1. On your management computer, start VMware vSphere Client.
2. In **IP address / Name**, type the IP address or FQDN of the VMware vSphere server.
3. In **User name**, type the name of your account on that server.
4. In **Password**, type the password for your account on that server.
5. Click *Login*.
6. In the pane on the left side, right-click the name of the virtual appliance, such as **FortiWeb-VM**, then select **Edit Settings**.

The virtual appliance's properties dialog appears.



7. In the list of virtual hardware on the left side of the dialog, click *Hard disk 2*.
8. In **Provisioned Size**, type the new size, in gigabytes (GB), of the vDisk.
9. Click **OK**.
10. If you do not need to change the other resources, continue with Powering on and shutting down the virtual appliance on page 45. Otherwise continue with Configuring the number of virtual CPUs (vCPUs) on page 32.
11. After powering on the appliance, in the CLI, enter the command:

```
exec formatlogdisk
```

On VMware ESXi, the expanded space will not be recognized **until** the vDisk is reformatted.

Configuring the number of virtual CPUs (vCPUs)

By default, the virtual appliance is configured to use 1 vCPU. Depending on the FortiWeb-VM license that you purchased, you can allocate up to 1, 2, 4, or 8 vCPUs.

If you need to increase or decrease the vCPUs after the initial boot, power off FortiWeb-VM, adjust the number of vCPUs, then see Updating the license for more vCPUs on page 155.

For FortiWeb-VM deployed on an ESXi hypervisor, when you set the number of vCPUs to 8, you also change the default CPU affinity settings (which restrict the virtual machines to a subset of the available processors). This additional configuration can help prevent performance problems.

For more information on vCPUs, see the VMware vSphere documentation:

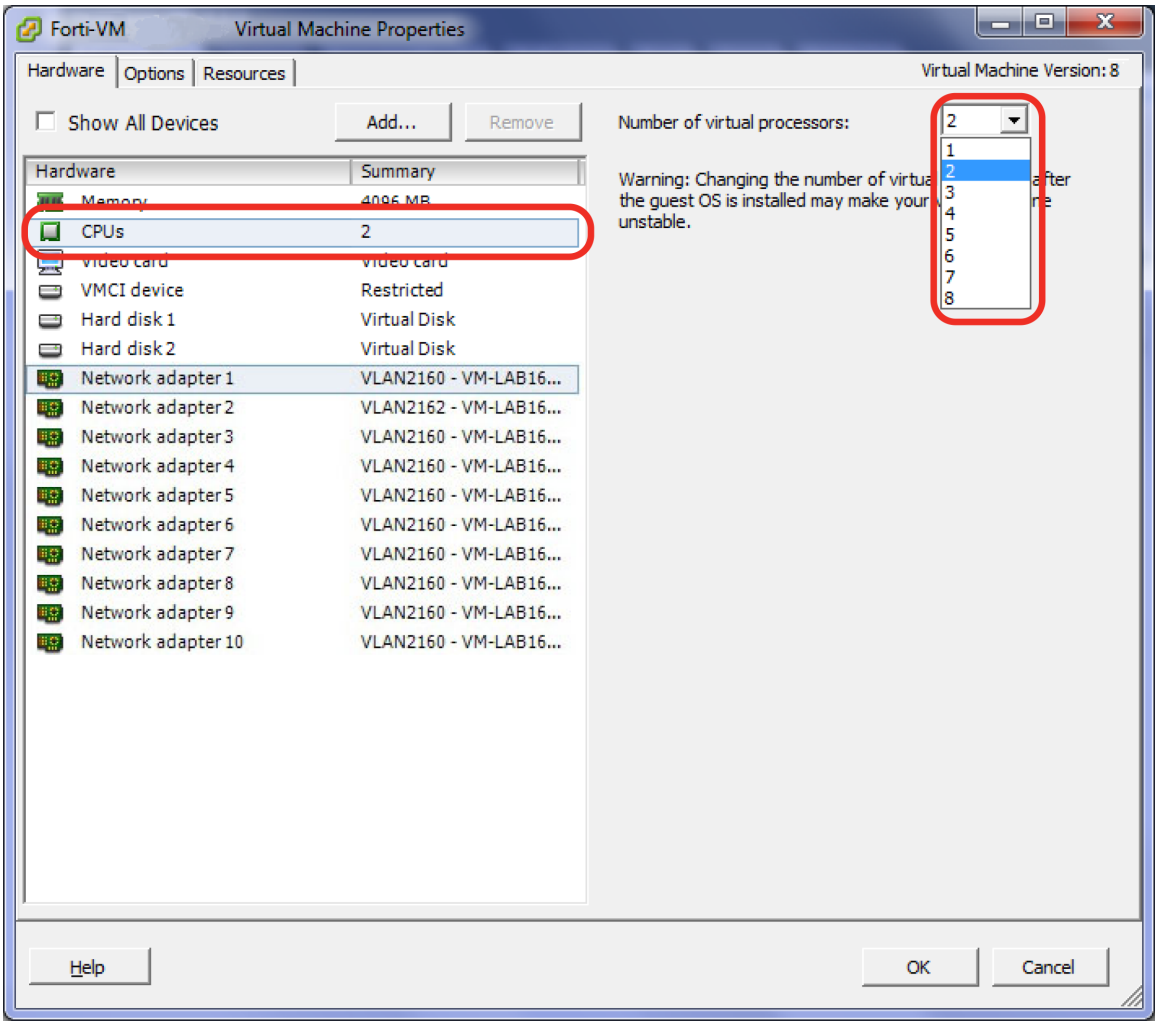
http://www.vmware.com/products/vsphere-hypervisor/index.html

To change the number of vCPUs

While resizing the vCPU, the FortiWeb-VM must be powered off.

1. On your management computer, start VMware vSphere Client.
2. In **IP address / Name**, type the IP address or FQDN of the VMware vSphere server.
3. In **User name**, type the name of your account on that server.
4. In **Password**, type the password for your account on that server.
5. Click *Login*.
6. In the pane on the left side, right-click the name of the virtual appliance, such as **FortiWeb-VM**, then select **Edit Settings**.

   The virtual appliance's properties dialog appears.
7. In the list of virtual hardware on the left side of the dialog, click *CPUs*.
8. In *Number of virtual processors*, type the maximum number of vCPUs to allocate. Valid values range from 1 to 8.



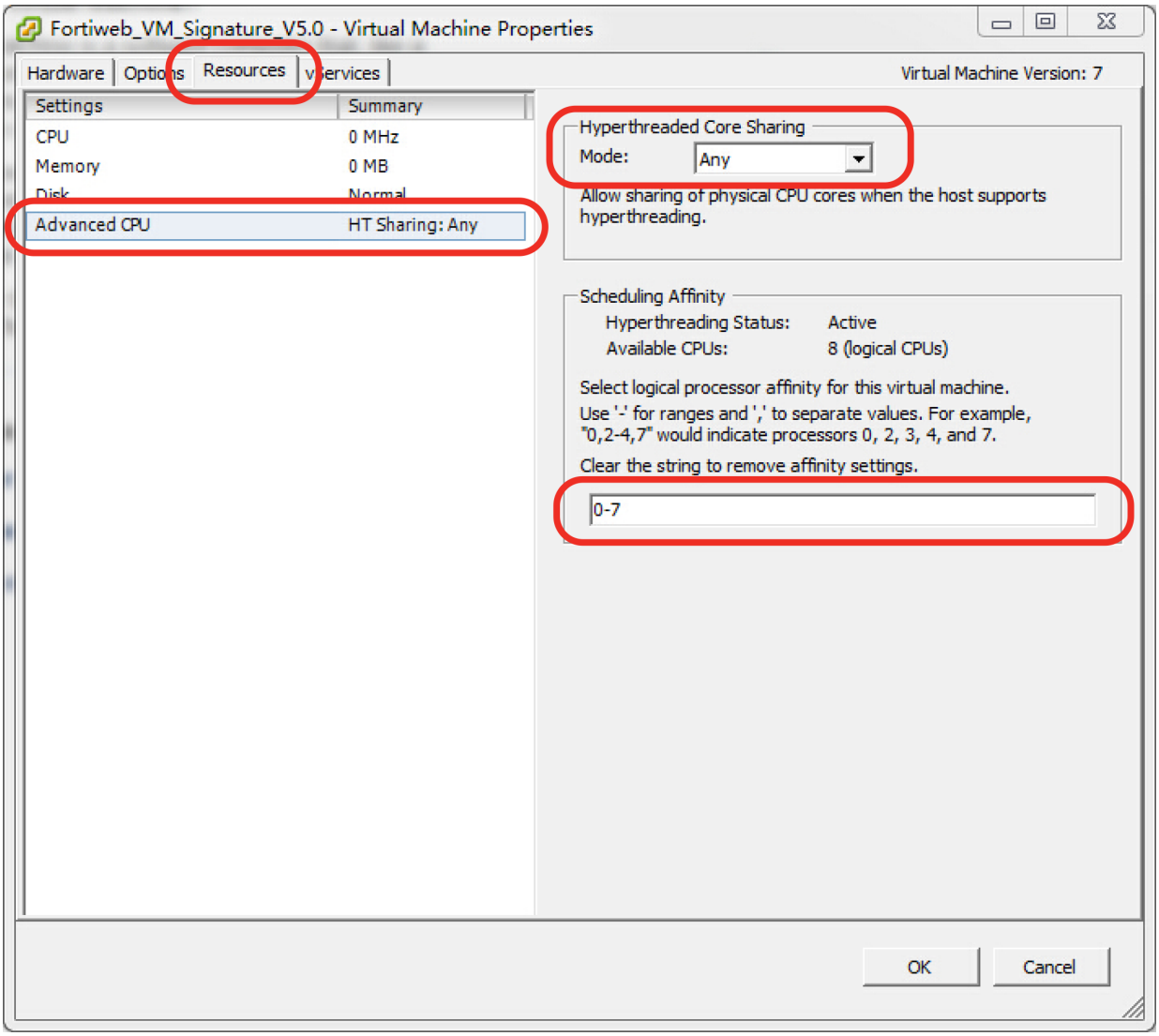
9. Click *OK*.
10. Do one of the following:
    - **For vSphere Hypervisor deployments and ESXi deployments with 2 or 4 vCPUs** – If you do not need to change the other resources, continue with Powering on and shutting down the virtual appliance on page 45. Otherwise continue with Configuring the virtual RAM (vRAM) limit on page 34.
    - **For ESXi deployments with 8 vCPUs** – Continue with the instructions in To configure vCPUs for FortiWeb-VM08 on ESXi on page 33

To configure vCPUs for FortiWeb-VM08 on ESXi

1. On VMware vSphere Client, ensure you are logged in to the VMware vSphere server.
2. Right-click the name of the virtual appliance, such as **FortiWeb-VM**, then select **Edit Settings**.

   The virtual appliance's properties dialog appears.
3. On the Resources tab, click *Advanced CPU*.
4. Under Hyperthreaded Core Sharing, for **Mode**, select **Any**.

5. Under Scheduling Affinity, to set the logical processor affinity to the required range, enter `0-7`.



6. If you do not need to change the other resources, continue with Powering on and shutting down the virtual appliance on page 45. Otherwise continue with Configuring the virtual RAM (vRAM) limit on page 34

Configuring the virtual RAM (vRAM) limit

FortiWeb-VM comes pre-configured to use 4 GB of vRAM. You can change this value.

It is possible to configure FortiWeb-VM to use less vRAM, such as 2 GB. However, for performance reasons, it is not recommended.

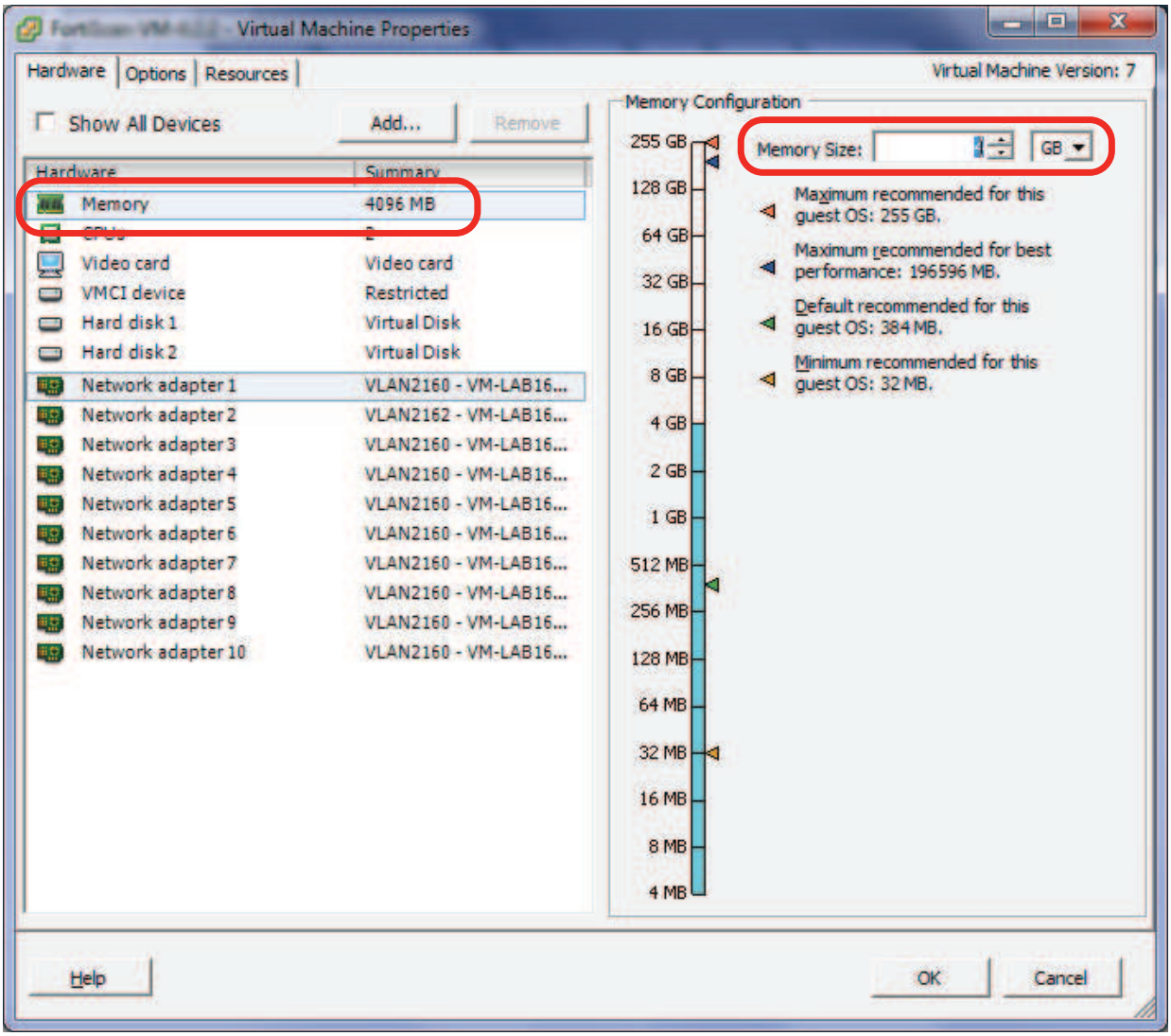
To change the amount of vRAM

While resizing the vRAM, the FortiWeb-VM must be powered off.

1. On your management computer, start VMware vSphere Client.
2. In **IP address / Name**, type the IP address or FQDN of the VMware vSphere server.
3. In **User name**, type the name of your account on that server.
4. In **Password**, type the password for your account on that server.
5. Click *Login*.
6. In the pane on the left side, right-click the name of the virtual appliance, such as **FortiWeb-VM**, then select **Edit Settings**.

   The virtual appliance's properties dialog appears.
7. In the list of virtual hardware on the left side of the dialog, click *Memory*.

8. In *Memory Size*, type the maximum number in gigabytes (GB) of the vRAM to allocate.



9. Click **OK**.

10. If you do not need to change the other resources, continue with Powering on and shutting down the virtual appliance on page 45. Otherwise continue with Mapping the virtual NICs (vNICs) to physical NICs on page 36.

Mapping the virtual NICs (vNICs) to physical NICs

Appropriate mappings of the FortiWeb-VM network adapter ports to the host computer's physical ports depends on your existing virtual environment.

Often, the default bridging vNICs work, and don't need to be changed.

If you are unsure of your network mappings, try bridging first **before** non-default vNIC modes such as NAT or host-only networks. The default bridging vNIC mappings are appropriate where each of the host's guest virtual machines should have their own IP addresses on your network.

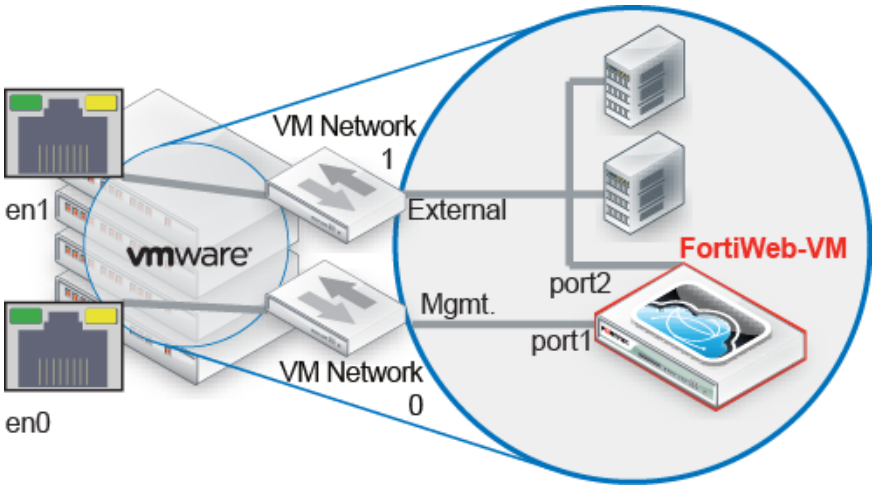
The most common exceptions to this rule are for VLANs and the transparent modes. See Configuring the vNetwork for the transparent modes on page 40

When you deploy the FortiWeb-VM package, 10 bridging vNICs are created and automatically mapped to a port group on 1 virtual switch (vSwitch) within the hypervisor. Each vNIC is mapped to one of 10 FortiWeb-VM network interfaces. (Alternatively, you can configure some or all of the network interfaces to use the same vNIC.) vSwitches are themselves mapped to physical ports on the server.

In some cases, FortiWeb-VM deployed on ESXi cannot update the mapping between vNICs and FortiWeb-VM network interfaces after you remove and add adaptors. See Changing the default network adaptors for EXSi deployments on page 39.

You can change the mapping, or map other vNICs, if either your VM environment requires it or FortiWeb-VM will be operating in either true transparent proxy or transparent inspection mode. (For information on how to choose the operation mode, see the setup instructions in the *FortiWeb Administration Guide*.)

The following table provides an example of how vNICs could be mapped to the physical network ports on a server.



Example: Network mapping for reverse proxy mode

VMware vSphere			FortiWeb-VM
Physical Network Adapter	**Network Mapping (vSwitch Port Group)**	**Virtual Network Adapter for FortiWeb-VM**	**Network Interface Name in Web UI/CLI**

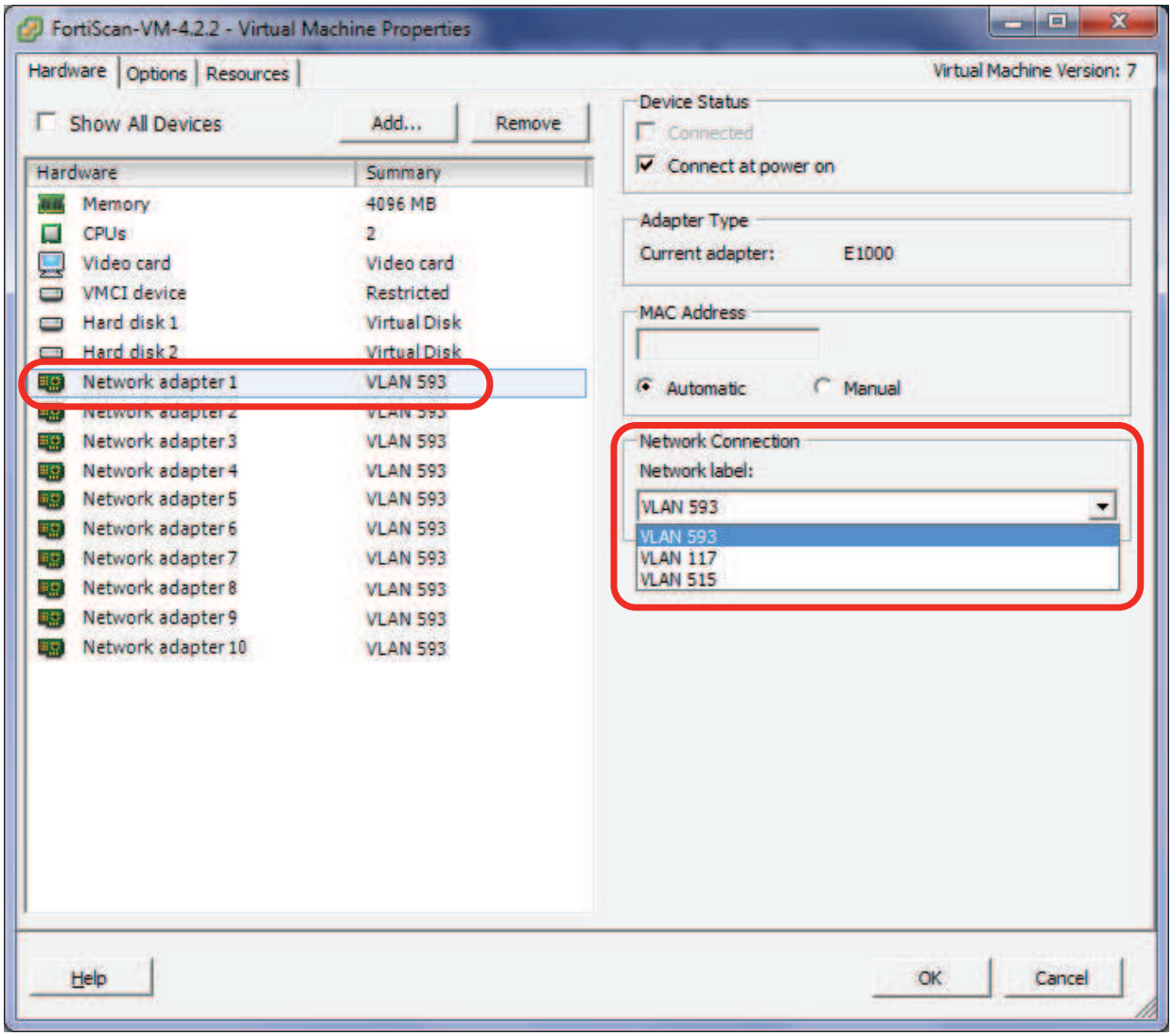
eth0	VM Network 0	Management	port1
eth1	VM Network 1	External	port2
	VM Network 2	Internal	port3
	VM Network 1	External	port4

To map network adapters

1. On your management computer, start VMware vSphere Client.
2. Enter the IP address, user name, and password of the VMware vSphere server.
3. Click *Login*.
4. In the pane on the left side, right-click the name of the virtual appliance, such as **FortiWeb-VM**, then select **Edit Settings**.

   The virtual appliance's properties dialog appears.
5. In the list of virtual hardware on the left side of the dialog, click the name of a virtual network adapter to see its current settings.
6. From the **Network Connection** drop-down menu, select the virtual network mapping for the virtual network adapter.

   The correct mapping varies by your virtual environment's network configuration. In the example illustration below, the vNIC **Network adapter 1** is mapped to the virtual network (vNetwork) named **VLAN 593.**



7. Click **OK**.
8. Continue with Powering on and shutting down the virtual appliance on page 45.

Changing the default network adaptors for EXSi deployments

By default, FortiWeb-VM deploys on ESXi using VMXNET network adaptors.

However, you can delete the VMXNET adaptors and add E1000 network adaptors that replace them, if required. E1000 adaptors do not have the same limitations as VMXNET adaptors. However, for best performance, use VMXNET adaptors because they are optimized for performance in a virtual machine.

To avoid problems with the mapping of vNICs to FortiWeb-VM network interfaces, do the following:

- Ensure the network adaptors are all of the same type: VMXNET or E1000.
- If you are using VMXNET adaptors, do not remove and add adaptors. FortiWeb-VM cannot update the initial mappings to work with the new adaptors.

  However, you can add VMXNET adaptors if you are upgrading from a previous version of FortiWeb-VM that

provides only 4 adaptors. (Because the additional adaptors are new, there is no existing mapping to create a conflict.) Ensure that the total number of adaptors after the upgrade is 8 or 10.

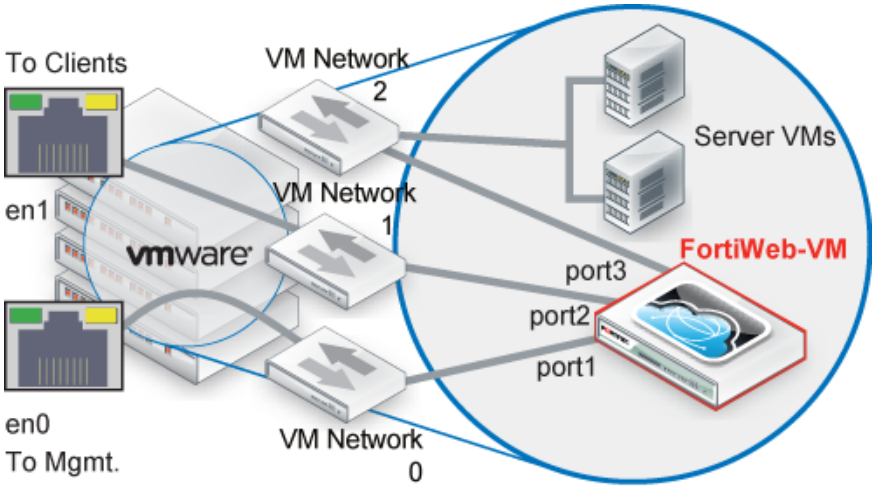
Configuring the vNetwork for the transparent modes

The default vNetwork configuration does **not** function with FortiWeb bridges (V-zones). You use bridges when you deploy your FortiWeb-VM in either true transparent proxy or transparent inspection operation mode.

Use the following general configuration steps to support the transparent modes:

- To create the bridge, use one of the following to create two FortiWeb ports: one for the web server side and one for the client side:
  - 2 vSwitches or distributed vSwitches (dvSwitch)
  - 1 vSwitch that has 2 port groups with different VLAN IDs
- Set each vSwitch that you add to promiscuous mode and map each port group to a network adapter (vNIC)

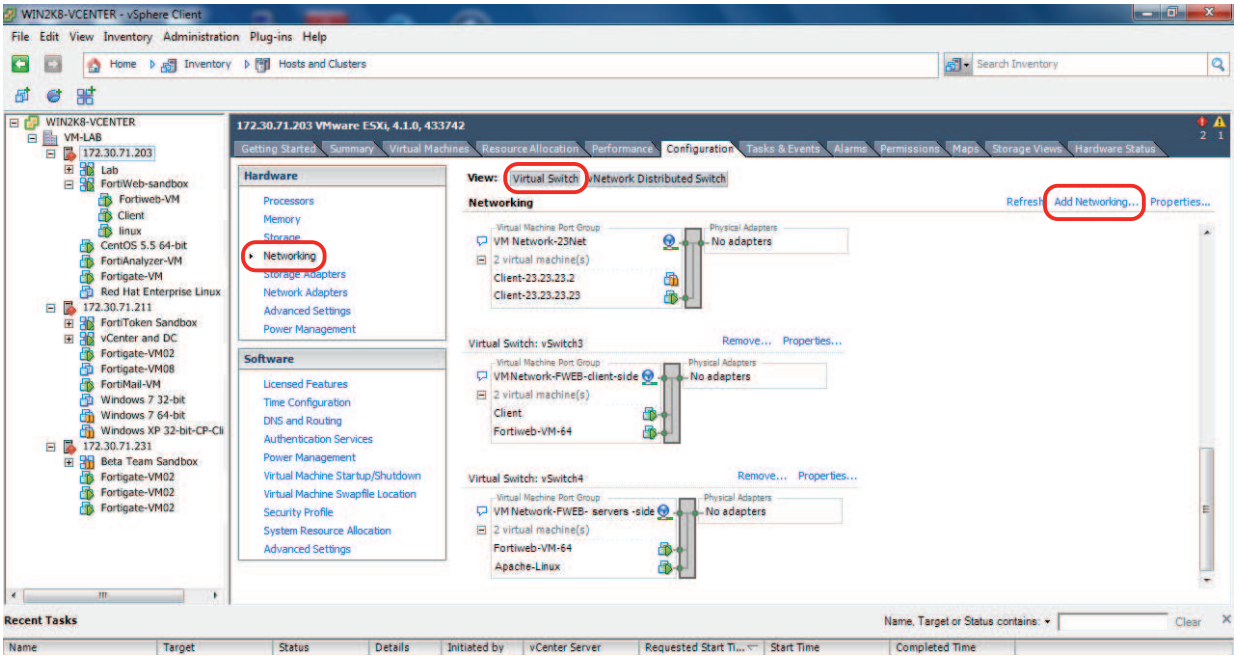
Similar to a deployment that does not use virtual machines, connections between clients and servers are piped through two port groups (on two vSwitches or a single vSwitch) that comprise the bridge, with FortiWeb-VM in between them.



To create a vSwitch

1. On your management computer, start VMware vSphere Client.
2. In **IP address / Name**, type the IP address or FQDN of the VMware vSphere server.
3. In **User name**, type the name of your account on that server.
4. In **Password**, type the password for your account on that server.
5. Click *Login*.
6. In the pane on the left side, click the name of the virtual appliance, such as **FortiWeb-VM**.
7. On the **Configuration** tab, click **Networking**.

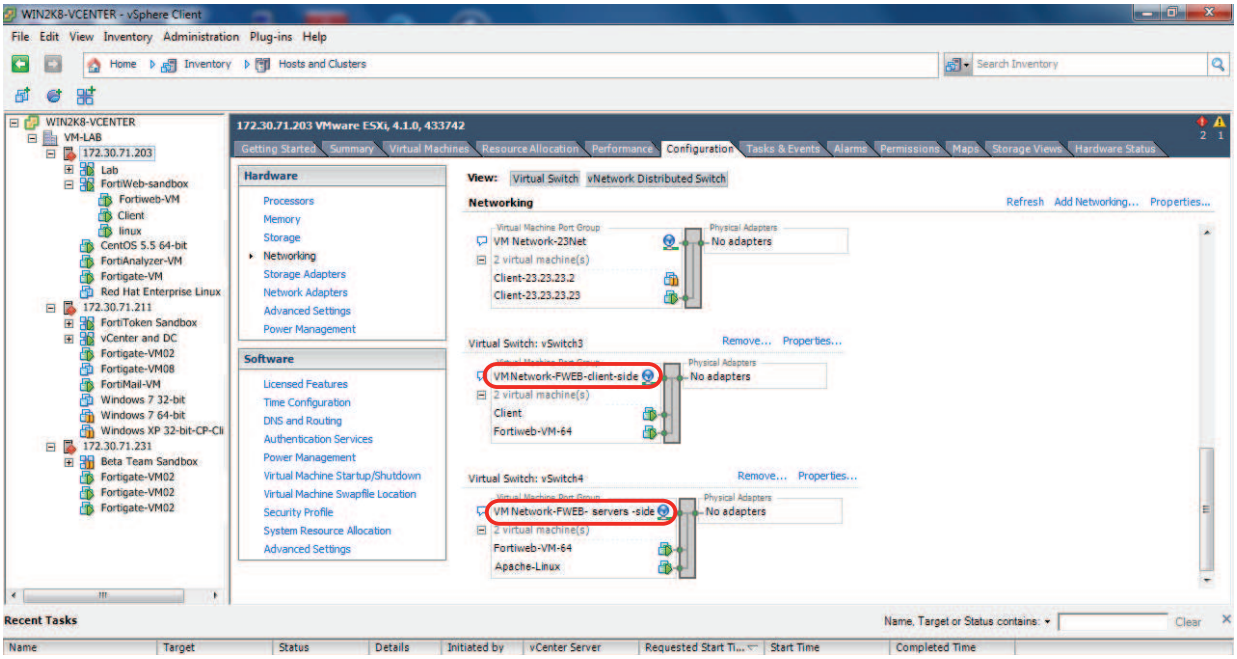
A window appears where you can configure vSwitches or distributed vSwitches.



8. In the **View** set of buttons, click **Virtual Switch**. (If you are configuring a distributed vSwitch, click **vNetwork Distributed Switch** instead. Your steps will vary slightly, but will be similar.)
9. Click **Add Networking**.
10. Accept the default connection type, **Virtual Machines**, and click **Next**.
11. Select **Create a virtual switch**.
12. Click **Next**.
13. Under **Port Group Properties**, enter a network label such as `Client-Side-vSwitch1` that identifies the port group.
14. In **VLAN ID**, if your network uses VLANs, enter a number between 1 and 4,094 to specify the VLAN tag that the vSwitch uses.

    If your configuration uses only one vSwitch, add a second port group with a different VLAN tag.
15. Click **Next**.
16. Click **Finish**.

17. If your configuration uses 2 vSwitches, repeat this procedure to create the other vSwitch.



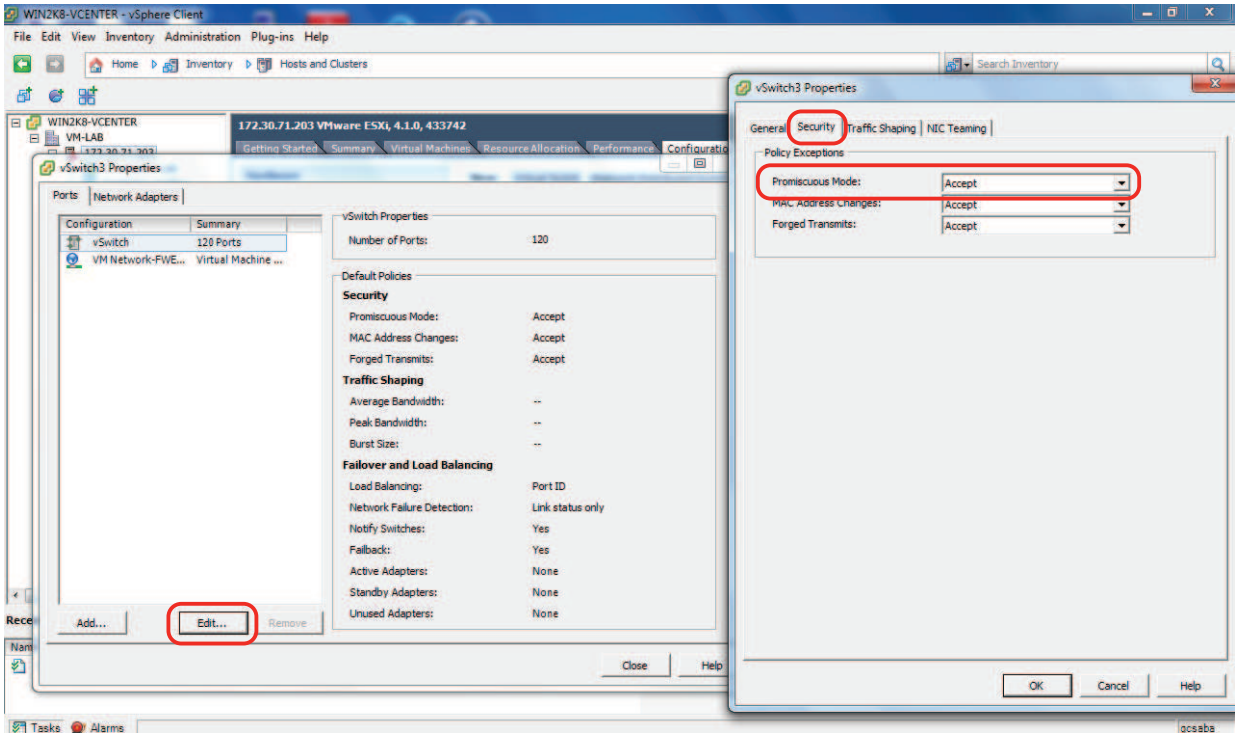
18. If you are creating vSwitches to support true transparent proxy, ensure that the vSwitch is configured to use only one VMNIC.

19. Continue with To configure promiscuous mode for the new vSwitch.

To configure promiscuous mode for the new vSwitch

1. On the **Configuration** tab, click **Networking**.

2. Select **Properties**.



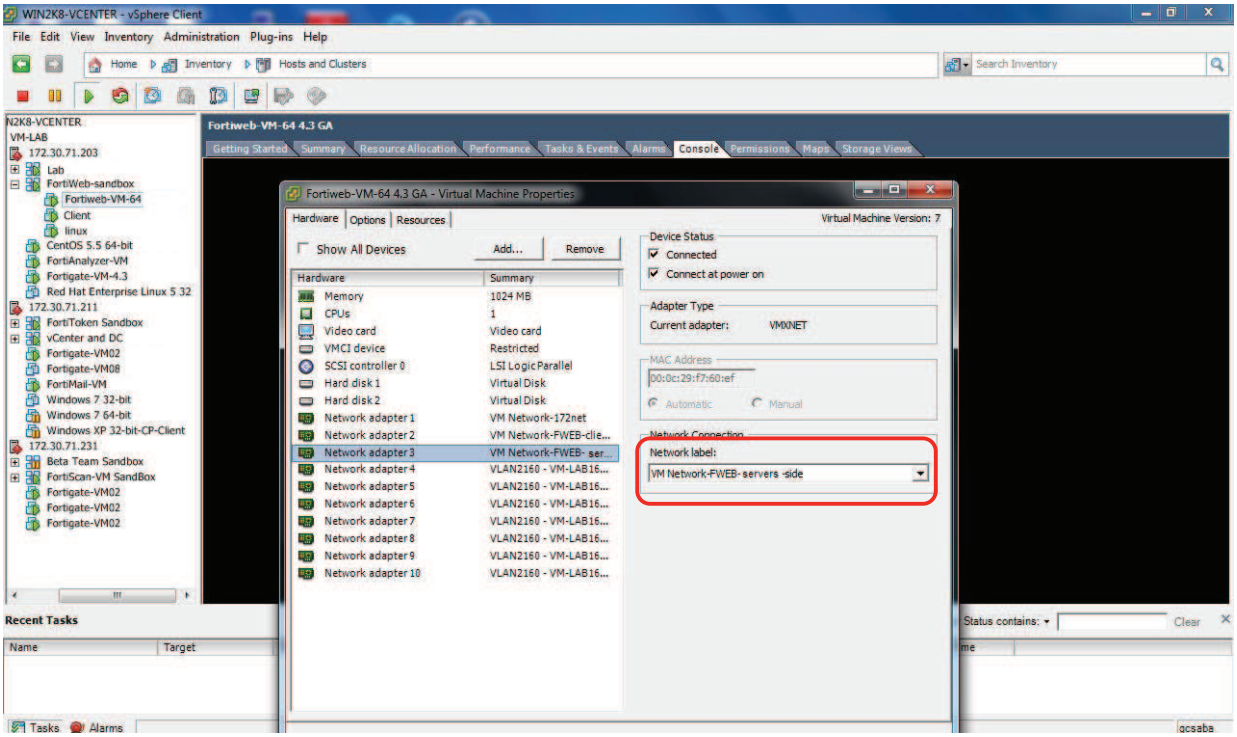
3. Click **Edit**.
4. Select the **Security** tab.
5. From the drop-down list for **Promiscuous Mode**, select **Accept.**
6. If your configuration uses 2 vSwitches, repeat this procedure with the other vSwitch for the bridge.
7. Continue with To map a network adapter to the new vSwitch port groups.

To map a network adapter to the new vSwitch port groups

1. In the pane on the left side, click the name of the virtual appliance, such as **FortiWeb-VM**.

2. On the **Getting Started** tab, select **Edit Virtual Machine Settings**.

A properties window appears.



3. On the **Hardware** tab, select a network adapter from the hardware list.

4. Select the port group of the new vSwitch from the **Network label** drop-down list.
5. Click **OK**.
6. Do one of the following:
   - If your configuration uses 2 vSwitches, repeat this procedure with the port group on the second vSwitch.
   - If your configuration users 1 vSwitch, repeat this procedure with the second port group on the vSwitch.
7. Later, when you configure FortiWeb-VM, add the FortiWeb ports that correspond to the mapped vSwitch port groups to the bridge (V-zone).

Configuring vSwitches to support an HA cluster on ESXi

To include FortiWeb-VM deployed on an ESXi hypervisor in a high availability (HA) cluster, ensure that the vSwitch **Promiscuous Mode**, **MAC Address Changes** and **Forged Transmits** security policies are all set to **Accept**.

This configuration allows the VM to become part of a cluster and process traffic correctly if there is a failover.

1. Log in to the vSphere Client and select the host from the inventory panel.
2. Click the **Configuration** tab and click **Networking**.
3. On the right side of the page, click **Properties** for the vSwitch to edit.
4. Click the **Ports** tab.
5. Select the vSwitch item in the Configuration list, and click **Edit**.
6. Click the **Security** tab.
7. For **Promiscuous Mode**, **MAC Address Changes** and **Forged Transmits**, select **Accept**.
8. Click **OK**.

Powering on and shutting down the virtual appliance

Once the virtual appliance's package has been deployed and its virtual hardware configured, you can power on the virtual appliance.

Do **not** power on the virtual appliance **unless** you have already mapped the virtual network adapter(s) (Mapping the virtual NICs (vNICs) to physical NICs on page 36). You may also want to:

- Resize disk (VMDK) (see Resizing the virtual disk (vDisk) on page 29)
- Configure the number of CPUs (see Configuring the number of virtual CPUs (vCPUs) on page 32)
- Set the RAM on virtual appliance (Configuring the virtual RAM (vRAM) limit on page 34)

These settings cannot be configured inside FortiWeb-VM, and must be configured in the virtual machine environment.

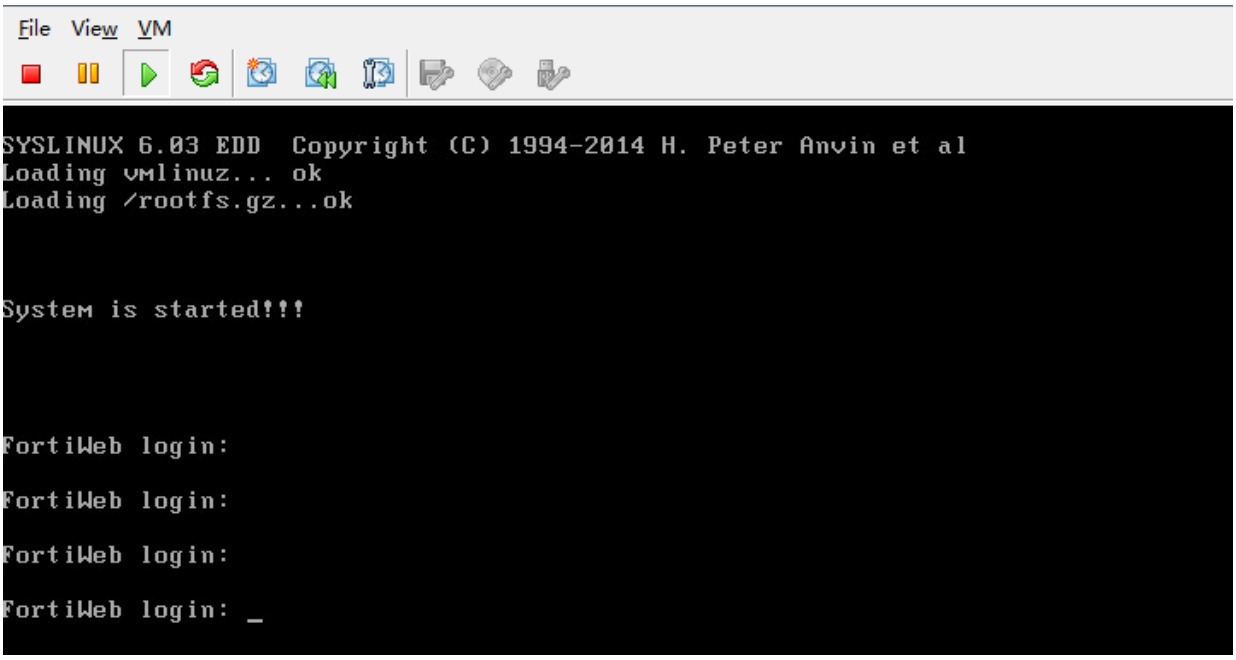
To power on FortiWeb-VM

1. On your management computer, start VMware vSphere Client.
2. In **IP address / Name**, type the IP address or FQDN of the VMware vSphere server.
3. In **User name**, type the name of your account on that server.
4. In **Password**, type the password for your account on that server.
5. Click *Login*.
6. In the pane on the left side, click the name of the virtual appliance, such as **FortiWeb-VM**.
7. Click the **Getting Started** tab.

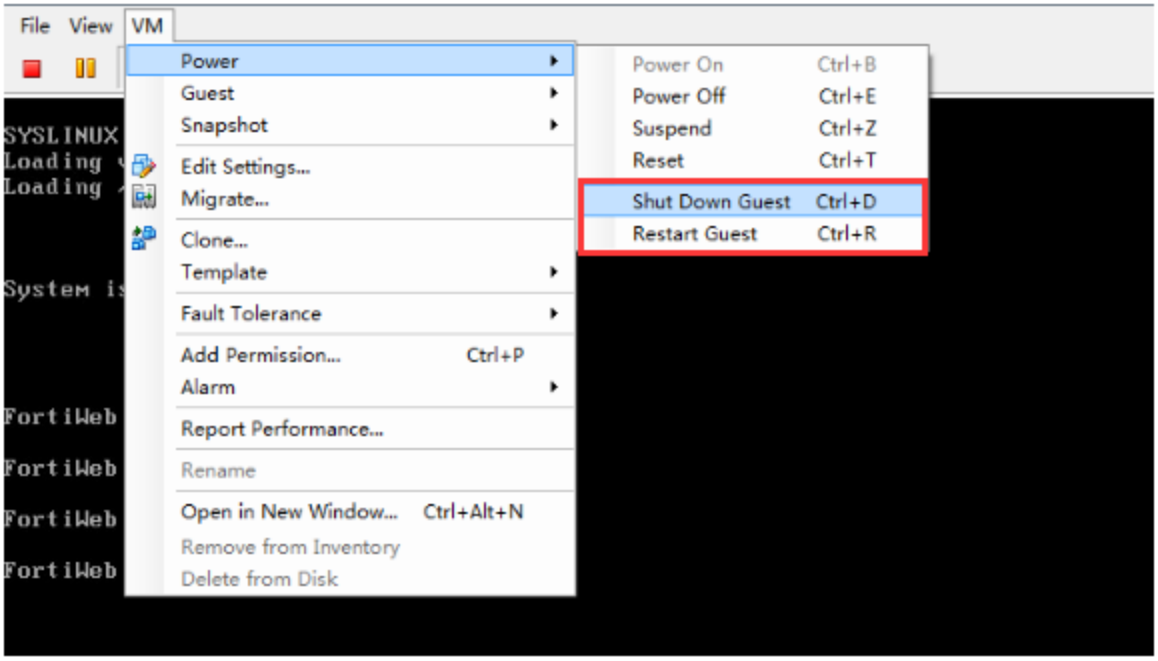
8. Click **Power on the virtual machine**.
9. Continue with Configuring access to FortiWeb's web UI & CLI on page 143.

To shut down or restart FortiWeb-VM

1. In the vSphere Client, access the FortiWeb-VM console.



2. Click **VM > Power**, and then select an option to shut down or restart the VM.



Configuring vSphere HA and Fault Tolerance

vSphere High Availability (HA) allows you to pool virtual machines and the hosts they reside on into a cluster. In the event of a failure, the HA feature restarts the virtual machines on a failed host on alternate hosts. This alternative to FortiWeb HA requires no HA configuration on the FortiWeb.

When you create a vSphere HA cluster, a single host automatically becomes the master host. The master host communicates with vCenter Server and monitors the state of all protected virtual machines and of the slave hosts.

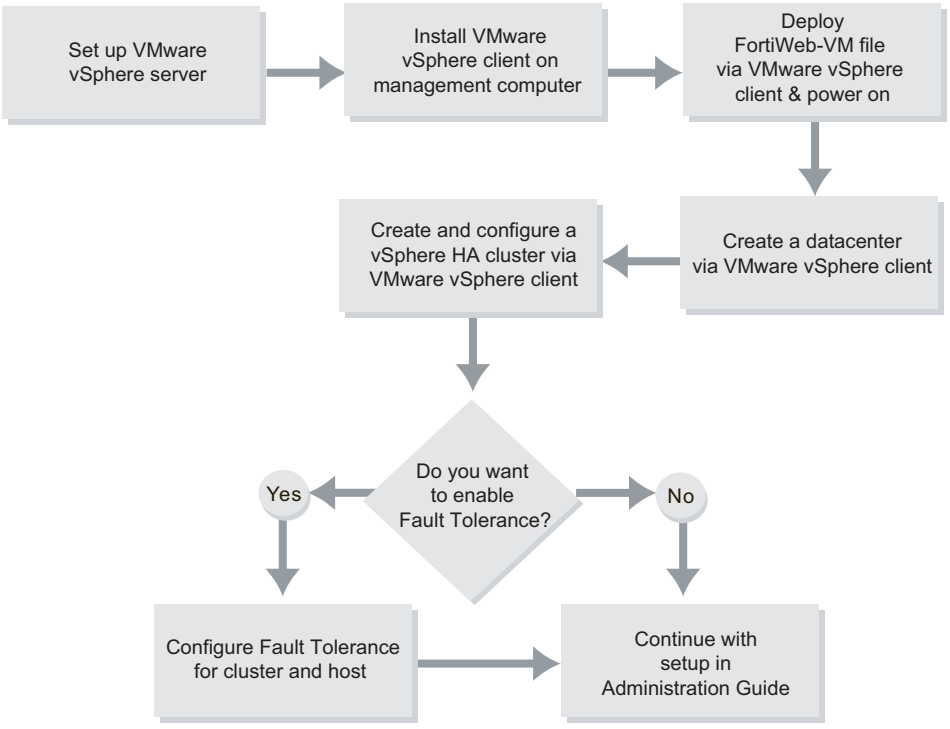
After you create a vSphere HA cluster, you can optionally enable Fault Tolerance (FT).

vSphere Fault Tolerance (FT) provides continuous availability by having identical virtual machines run in virtual lockstep on separate hosts. The lockstep mechanism captures activity and events on a primary virtual machine and sends them to a secondary VM.

To obtain optimal results from Fault Tolerance, ensure that you are familiar with how it works, how to enable it for your cluster and virtual machines, and FT best practices.

The key difference between VMware's Fault Tolerance and High Availability is how the failure of an ESXi host affects VM operation. Fault-tolerant systems instantly transition to a new host. For high-availability systems, the VMs fail with the host before restarting on another host.

Steps for configuring vSphere HA and Fault Tolerance



vSphere HA requirements

- VMware Infrastructure Suite Standard or Enterprise
- At least 2 VMware vSphere ESXi host systems
- A shared SAN or NAS between the ESXi servers where FortiWeb-VM is deployed. When a host system fails, ownership of its virtual machines is transferred from the failed host to the new host.
- CPU compatibility between the hosts

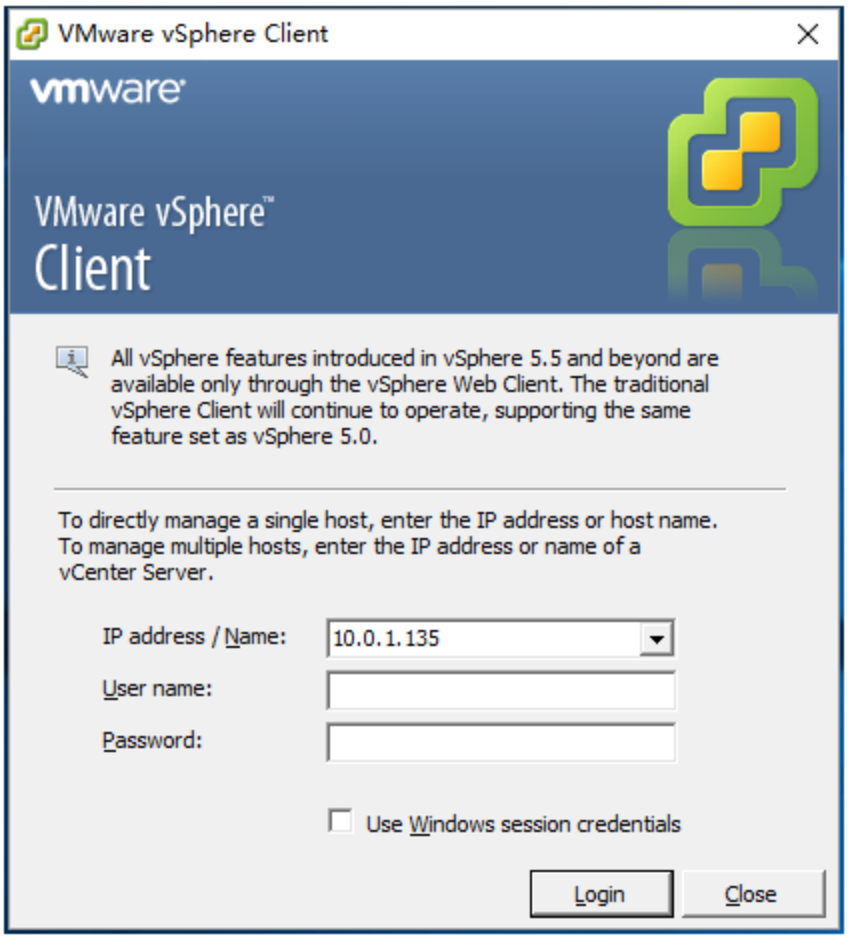
vSphere Fault Tolerance requirements

- Ensure the hosts use supported processors
- Ensure the hosts are licensed for Fault Tolerance
- Ensure the hosts are certified for Fault Tolerance. To determine if your hosts are certified, search the VMware Compatibility Guide by Fault Tolerant Compatible Sets.
- Ensure Hardware Virtualization (HV) is enabled in the BIOS for each host

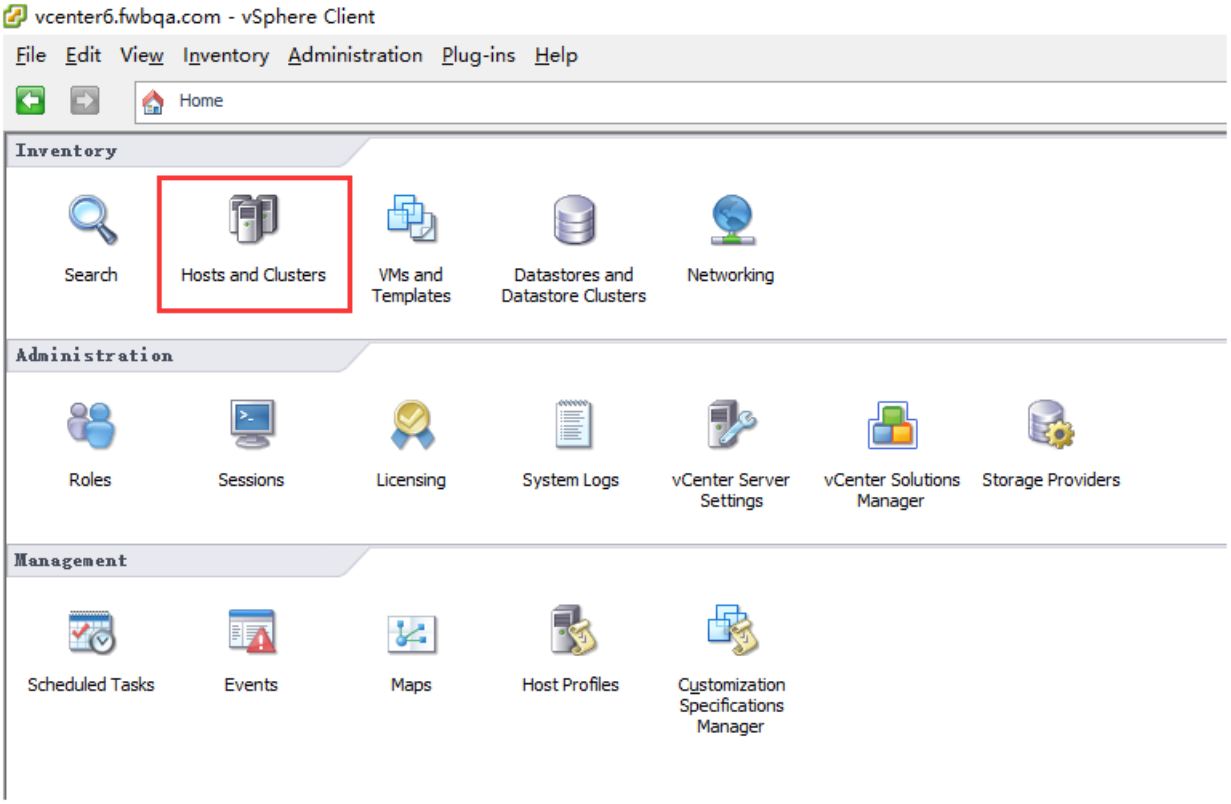
For more information on Fault Tolerance, see the topic "Providing Fault Tolerance for Virtual Machines" in ESXi and vCenter Server 5 Documentation.

To configure vSphere HA

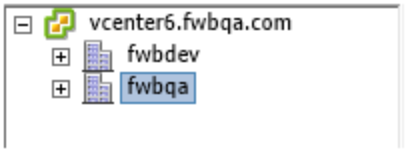
1. On your management computer, log in to VMware vSphere Client.



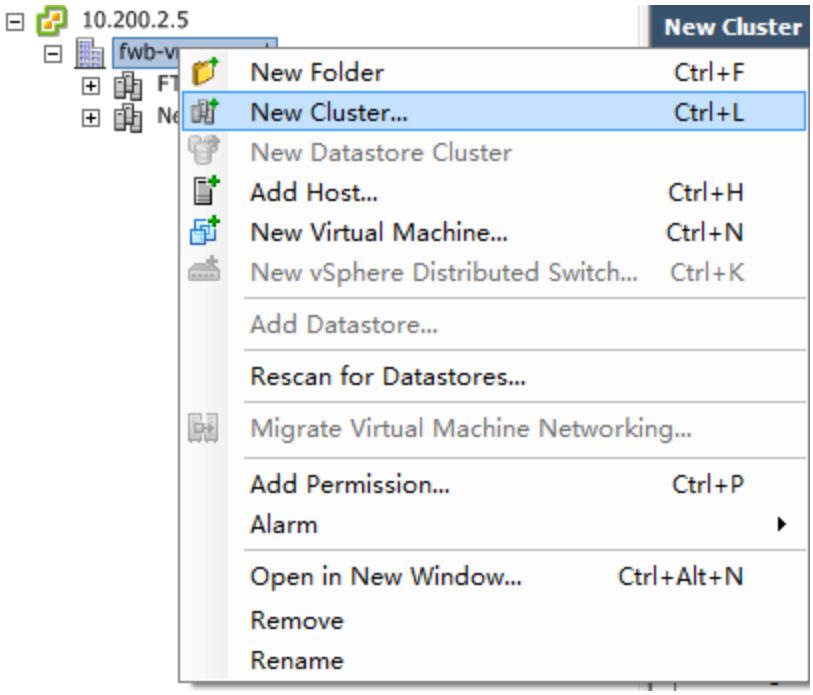
2. In the Home, under Inventory, click **Hosts and Clusters**.



3. Select **File > New > Datacenter**.
4. Rename the new datacenter. (In this example, it is `fwbqa`.)

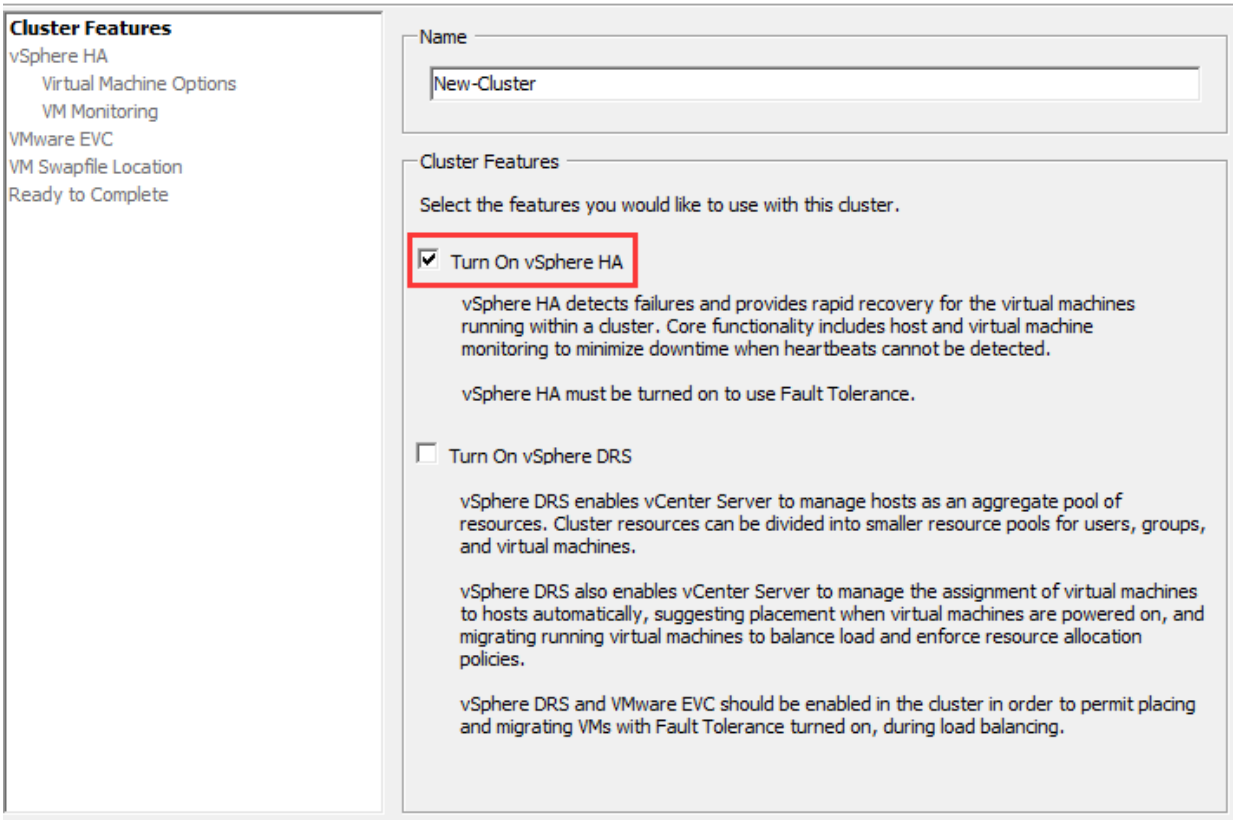


5. Right-click the datacenter, and then click **New Cluster**.



The New Cluster wizard is displayed.

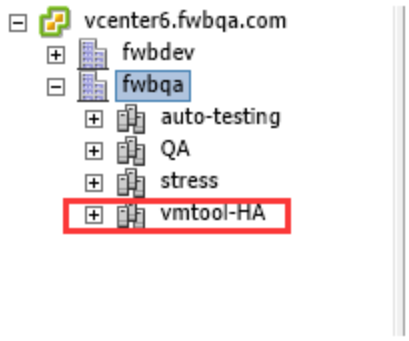
6. For **Name**, enter a name for the cluster, and then select **Turn On vSphere HA**.



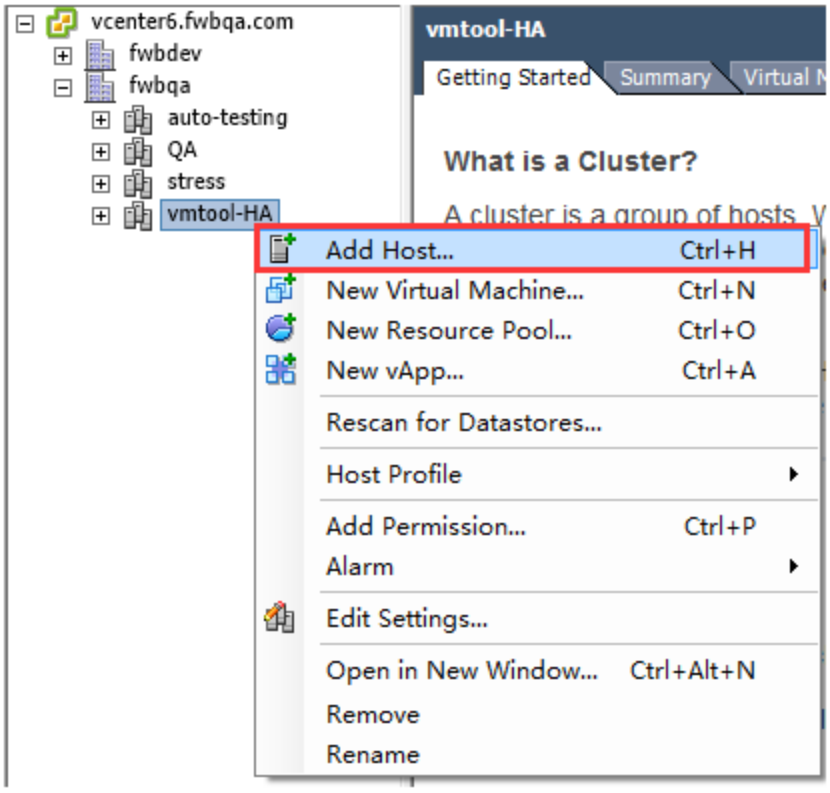
7. Navigate through the wizard to complete the configuration for your cluster.

   For information on the settings, see the topic "Configuring vSphere HA Cluster Settings" in ESXi and vCenter Server 5 Documentation.

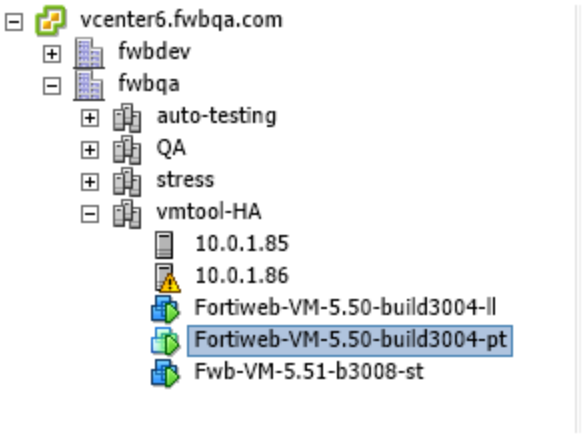
   The new cluster is displayed in the Inventory tree. (In this example, `vmtool-HA`.)



8. To add hosts to the cluster, right-click it, click **Add Host**.



9. Navigate through the wizard to add the hosts. (In this example, `10.0.1.85` and `10. 0.1.86`.)

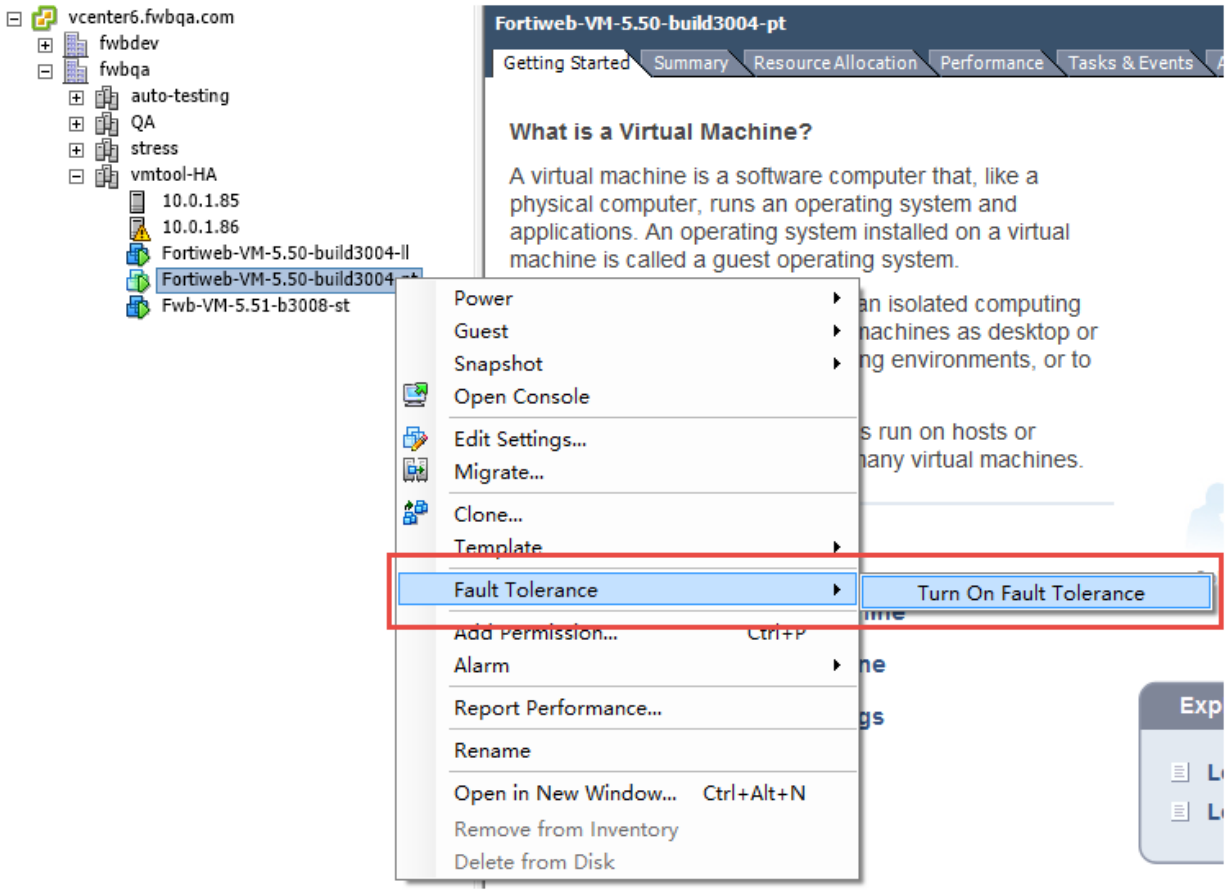


10. Select the cluster to view its settings and ensure that there are no configuration issues.

    For information on troubleshooting virtual machines, ESXi hosts, and clusters, see the topic "vSphere Troubleshooting" in ESXi and vCenter Server 5 Documentation.

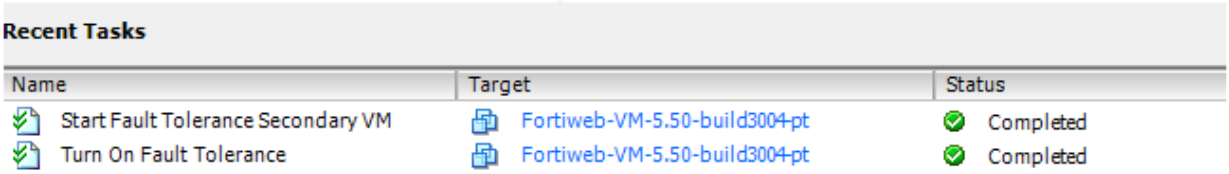
To configure vSphere FT

1. On your management computer, start VMware vSphere Client.
2. Right-click your virtual machine, and then click **Fault Tolerance > Turn On Fault Tolerance**.

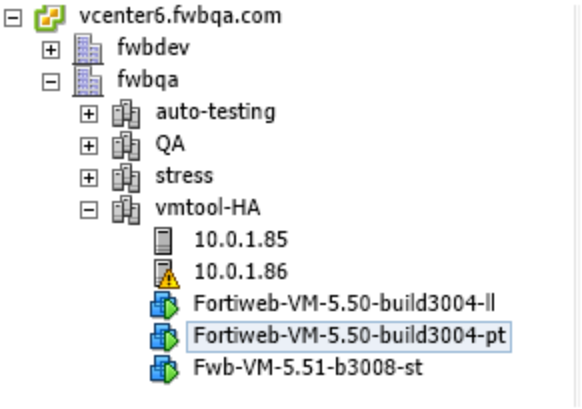


A confirmation dialog box is displayed.

3. Click **Yes** to confirm the feature activation.
4. Use the Recent Tasks panel to ensure there are no configuration issues.



The Inventory tree icons for VMs with FT are a different colour than VMs without FT.



Configuring vRealize Orchestrator

VMware vRealize Orchestrator is a development and process-automation tool that provides a library of extensible workflows. These workflows allow you to create and run automated, configurable processes to manage the VMware vSphere infrastructure as well as other VMware and third-party technologies. Orchestrator exposes vCenter Server API operations, which allows you to integrate them into your automated processes.

See the topics "Installing and Configuring VMware vRealize Orchestrator" and "Managing Workflows" in VMware vRealize Orchestrator 6.0 Documentation.

For example, you can create a workflow that modifies an existing virtual machine, including shutting down the guest operating system, renaming the machine, and modifying the memory. Go to the following location for more information:

www.vmwarebits.com/content/create-your-first-vcenter-orchestrator-workflow

VM Tools

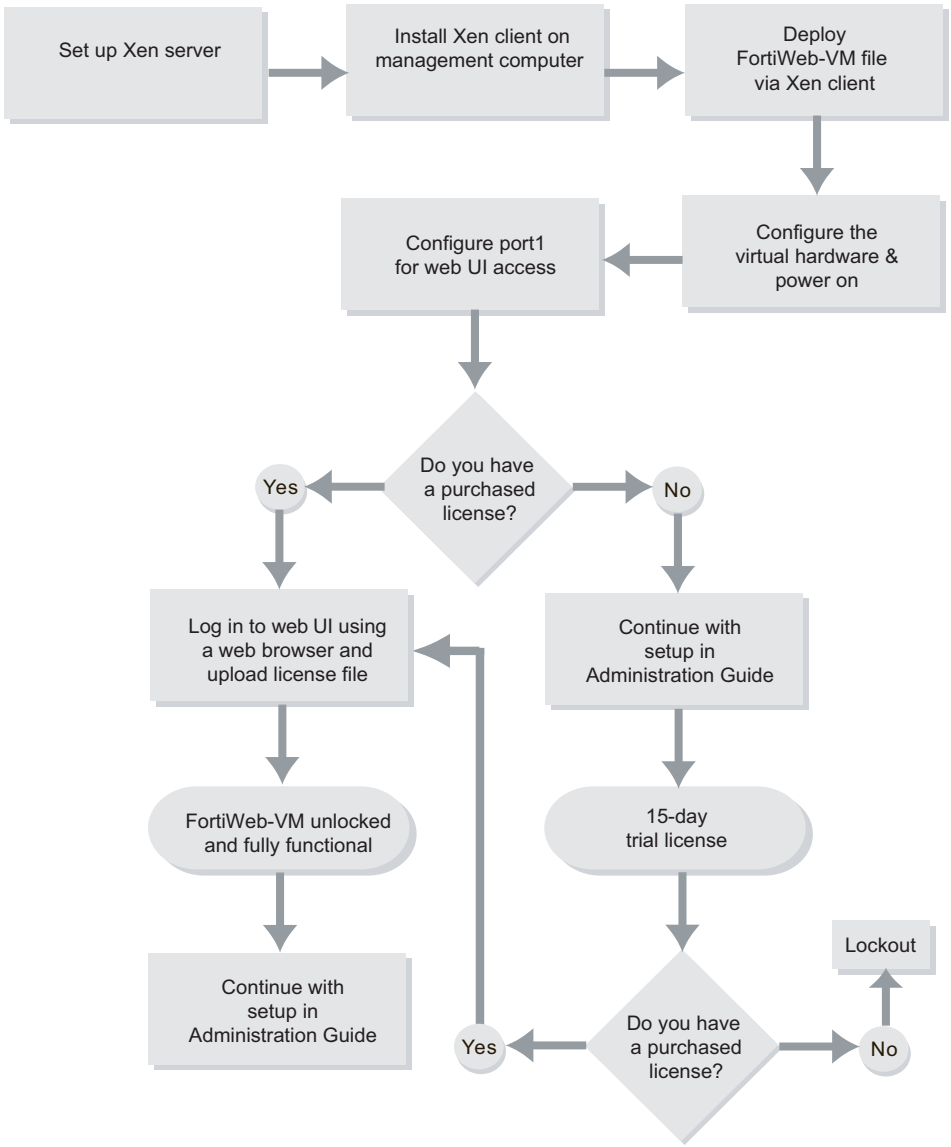
When you deploy FortiWeb-VM on VMware vSphere, VM Tools is installed with the virtual machine. VM Tools allows FortiWeb-VM to work with native vSphere functionality, such as vSphere HA and Fault Tolerance and guest system shutdown and restart.

However, because the version of VM Tools included with FortiWeb-VM is Open VM Tools, you cannot install or upgrade the tools using the **Install/Upgrade VMware Tools** option from the toolbar or vCenter server. Instead, updates are included with FortiWeb-VM updates.

Deploying FortiWeb-VM on Citrix Xen

The diagram below overviews the process for installing FortiWeb-VM on Citrix XenServer, which is described in the subsequent text.

Basic steps for installing FortiWeb-VM (Citrix XenServer)

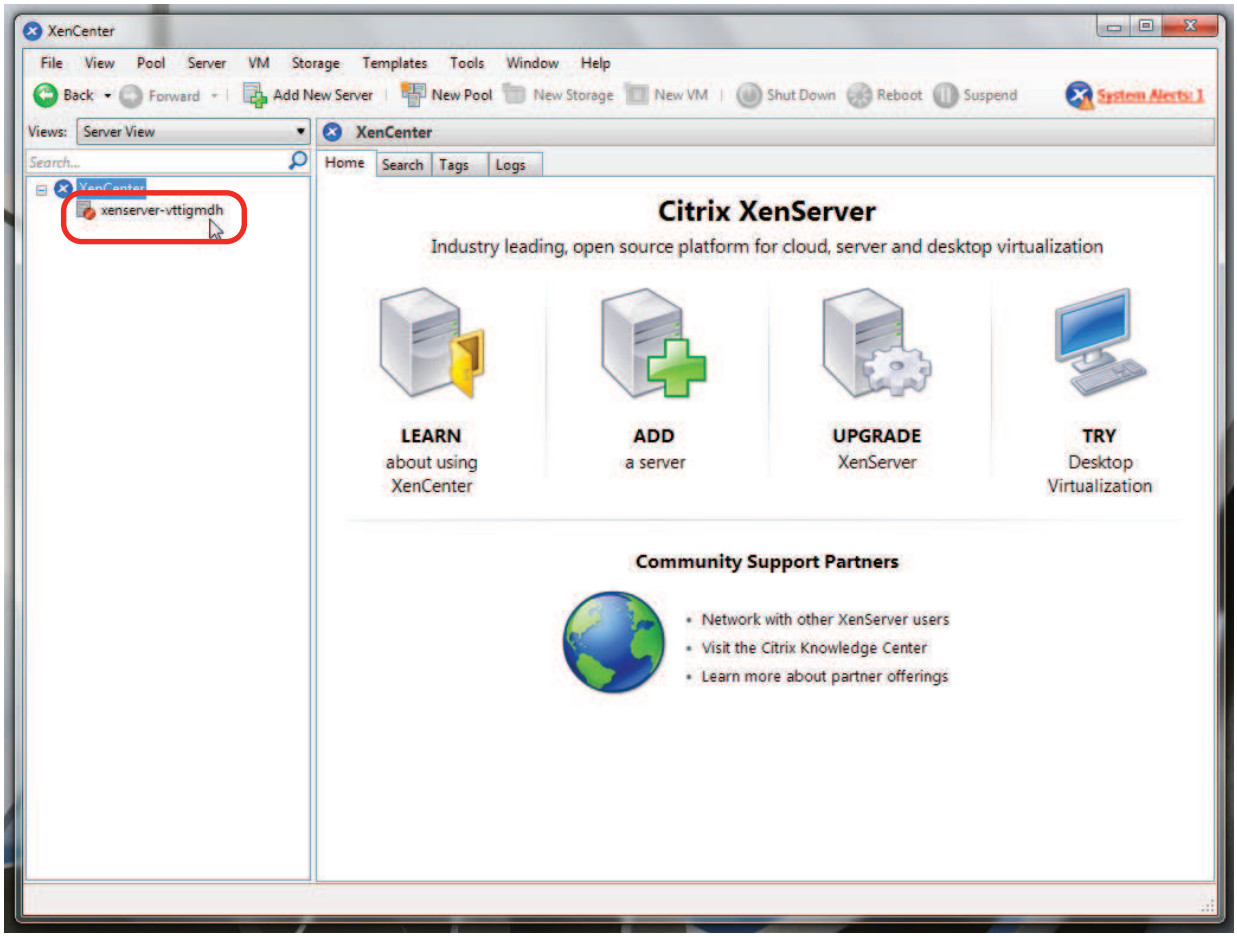


Deploying the OVF file

Before you can configure FortiWeb-VM, you must first use Citrix XenCenter to convert the open virtualization format (OVF) package to a format that can be used with Citrix XenServer, and to deploy the `FortiWeb-VM.ovf` template package.

To deploy the virtual appliance

1. On your management computer, start Citrix XenCenter.

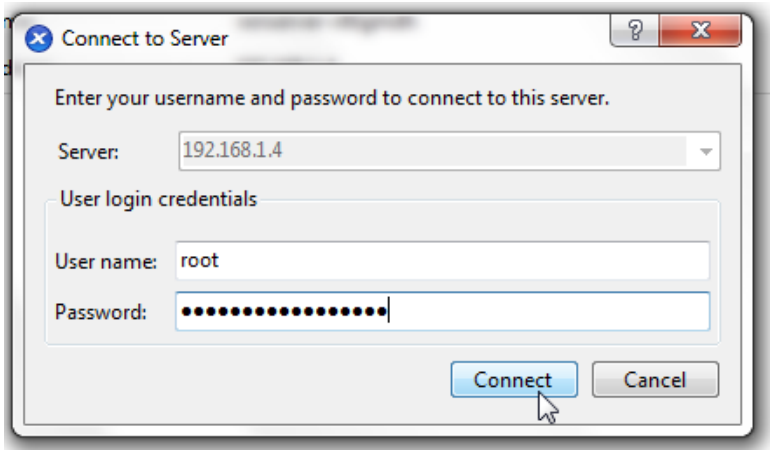


2. In the pane on the left side, double-click the name of the XenServer. This will open an authentication dialog.
3. In **Server**, type the IP address or FQDN of the Citrix XenServer server.

   In **User name**, type the name of your account on that server.

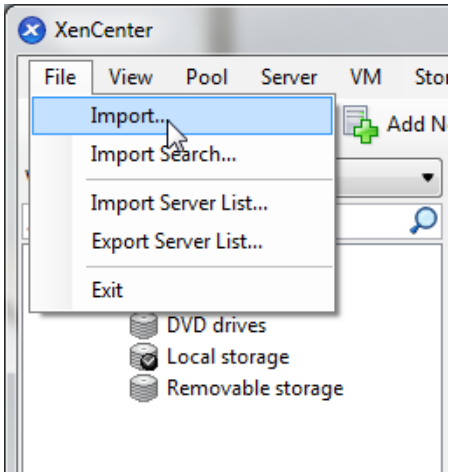
   In **Password**, type the password for your account on that server.

Click *Connect*.



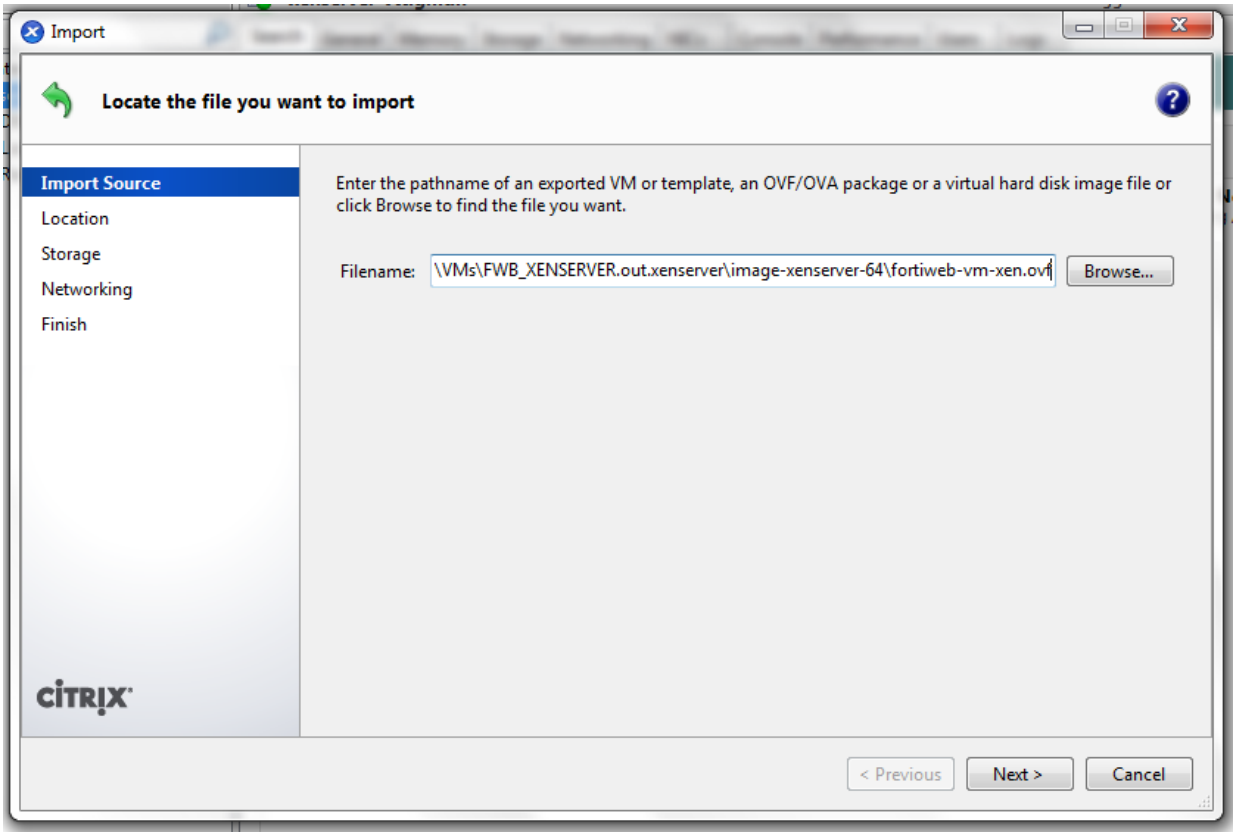
4. Go to **File > Import**. An import dialog will appear.

Alternatively, if you stored your downloaded FortiWeb-VM image in a centralized storage repository for images of new virtual machines, go to **Templates > Create VM From Selection**. After the VM template is deployed to your XenServer, subsequent steps such as adjusting allocated vCPUs are similar.

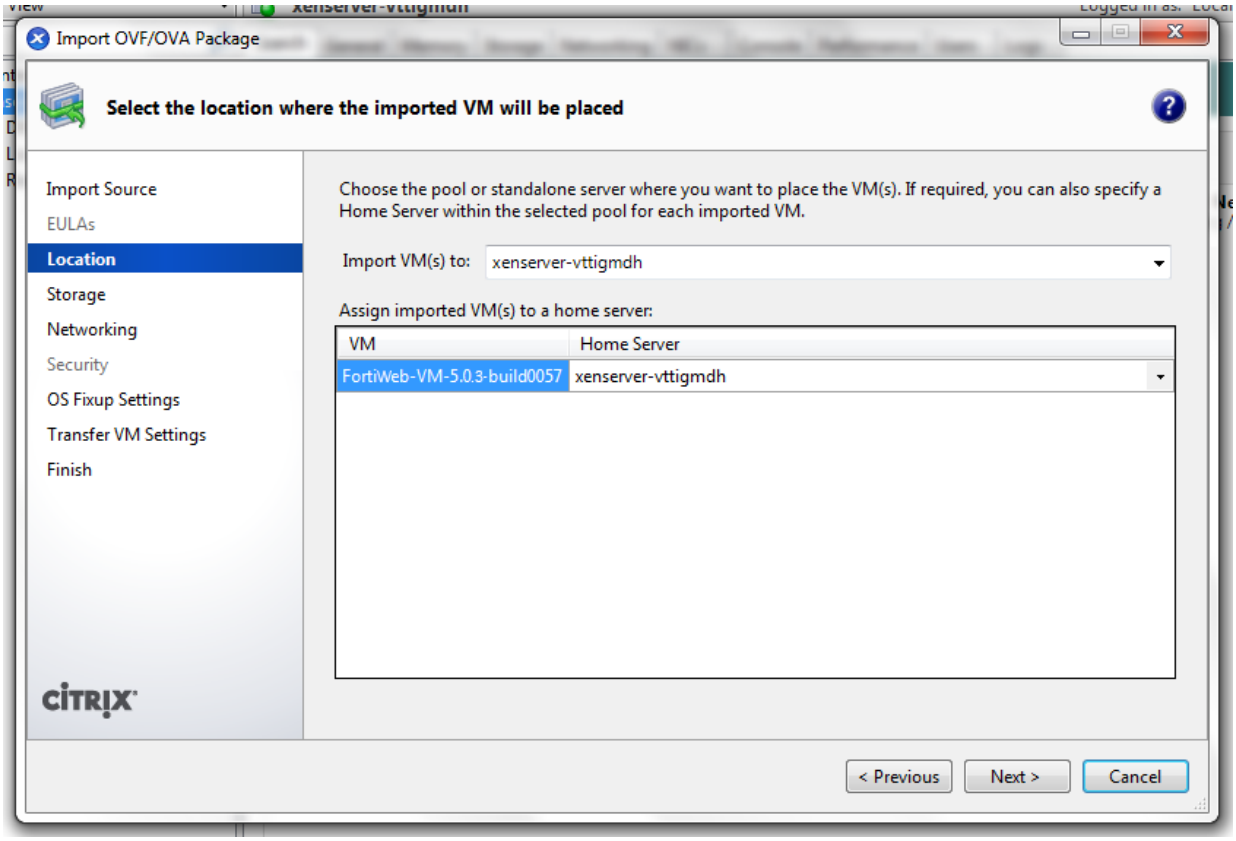


A deployment wizard window appears.

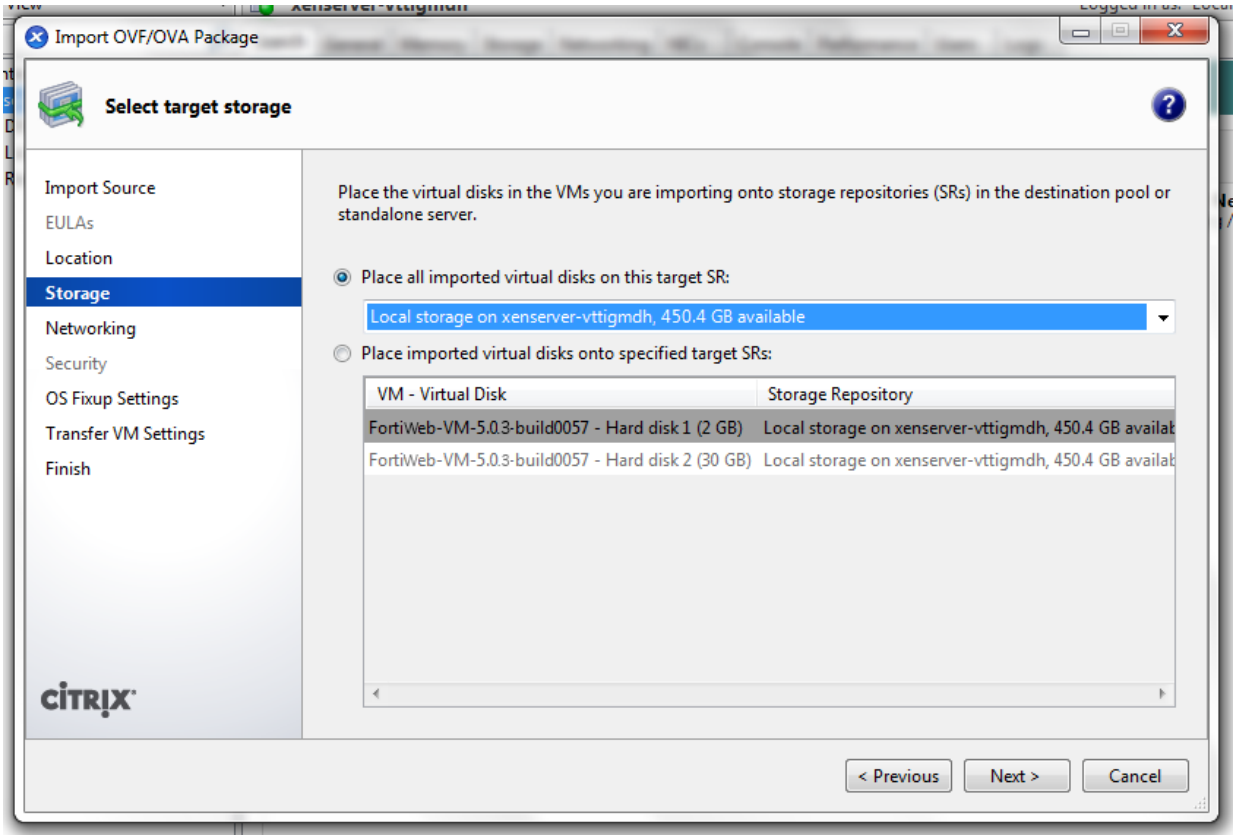
5. Click the **Browse** button to select the FortiWeb-VM.ovf template package, then click **Next**.



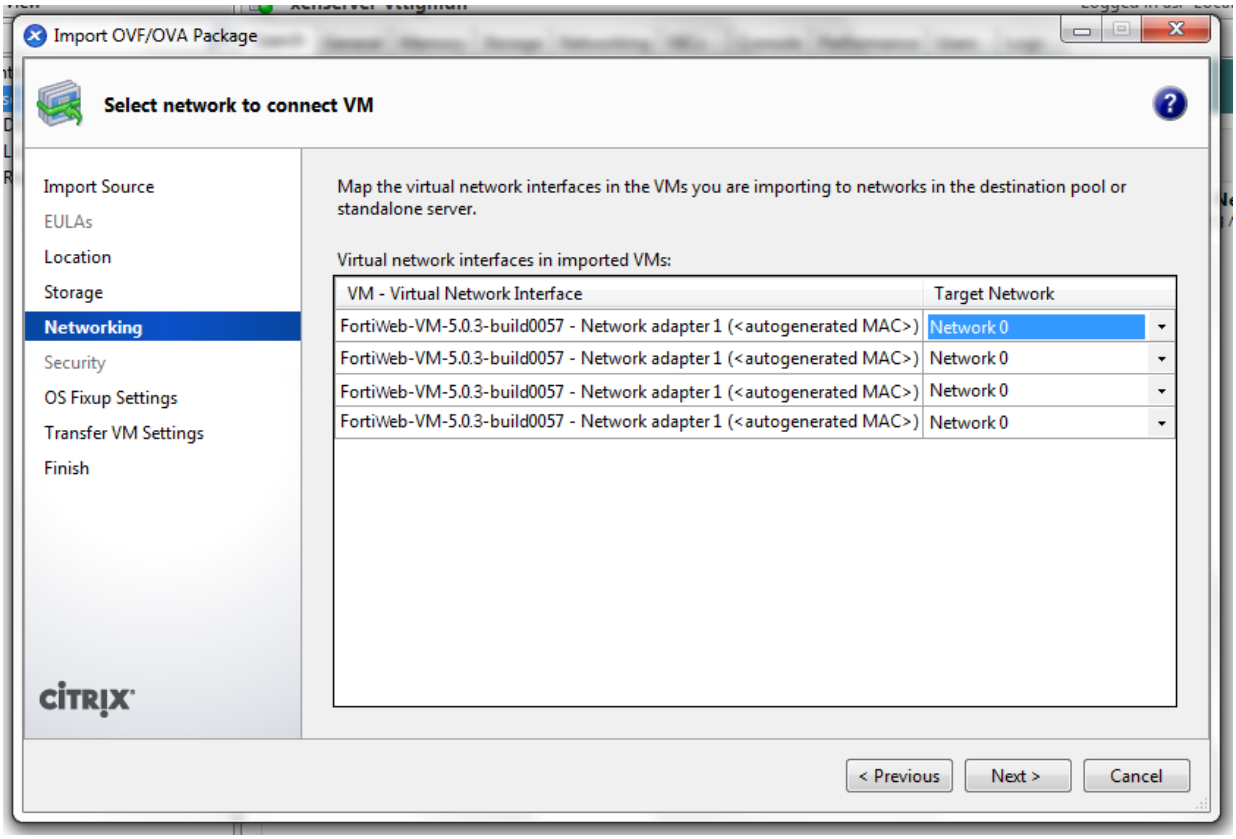
6. Confirm the XenServer where you want to deploy FortiWeb-VM, then click **Next**.



7. If you have multiple storage repositories, such as if you have an NFS or Windows (CIFS) share, select where the vDisks will be physically stored, then click **Next**.



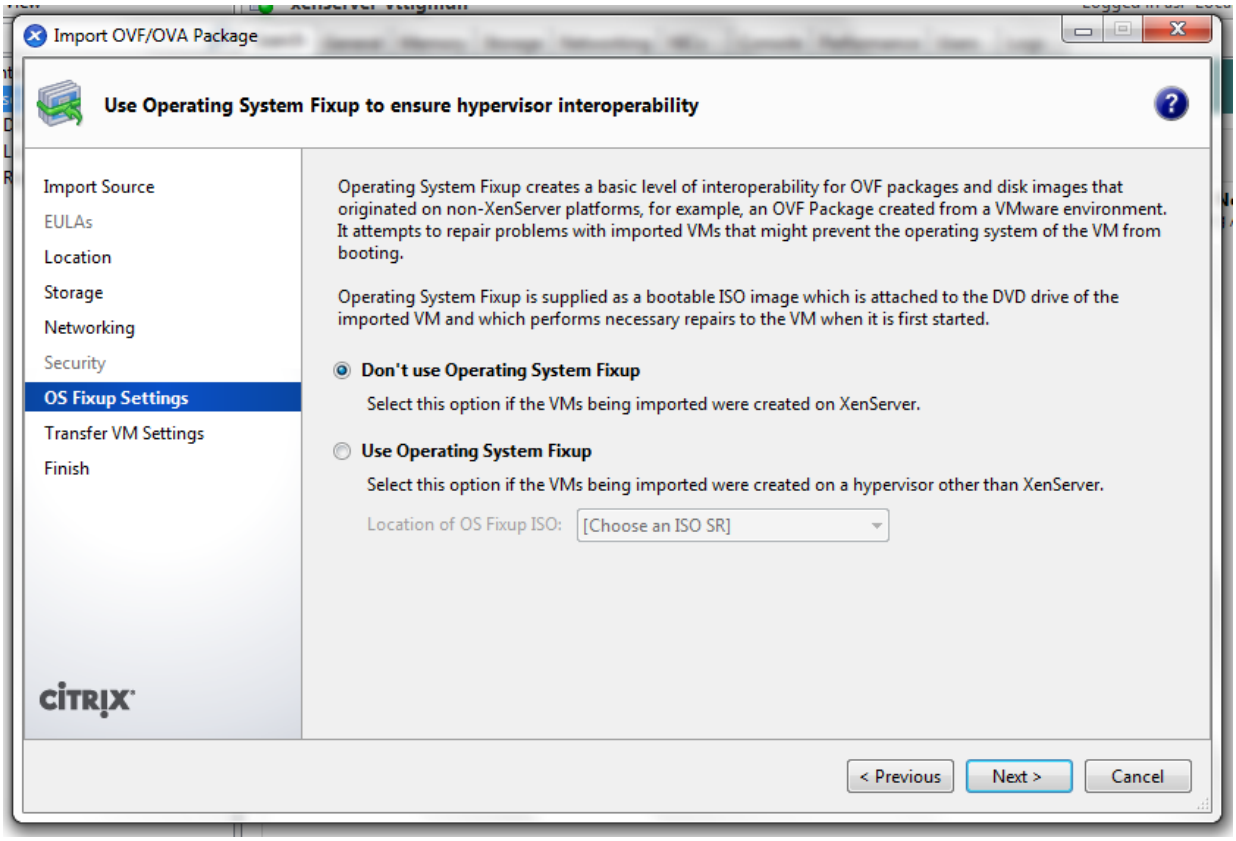
8. Configure how each vNIC (virtual network adapter) in FortiWeb-VM will be mapped to each vNetwork on that XenServer, then click **Next**.



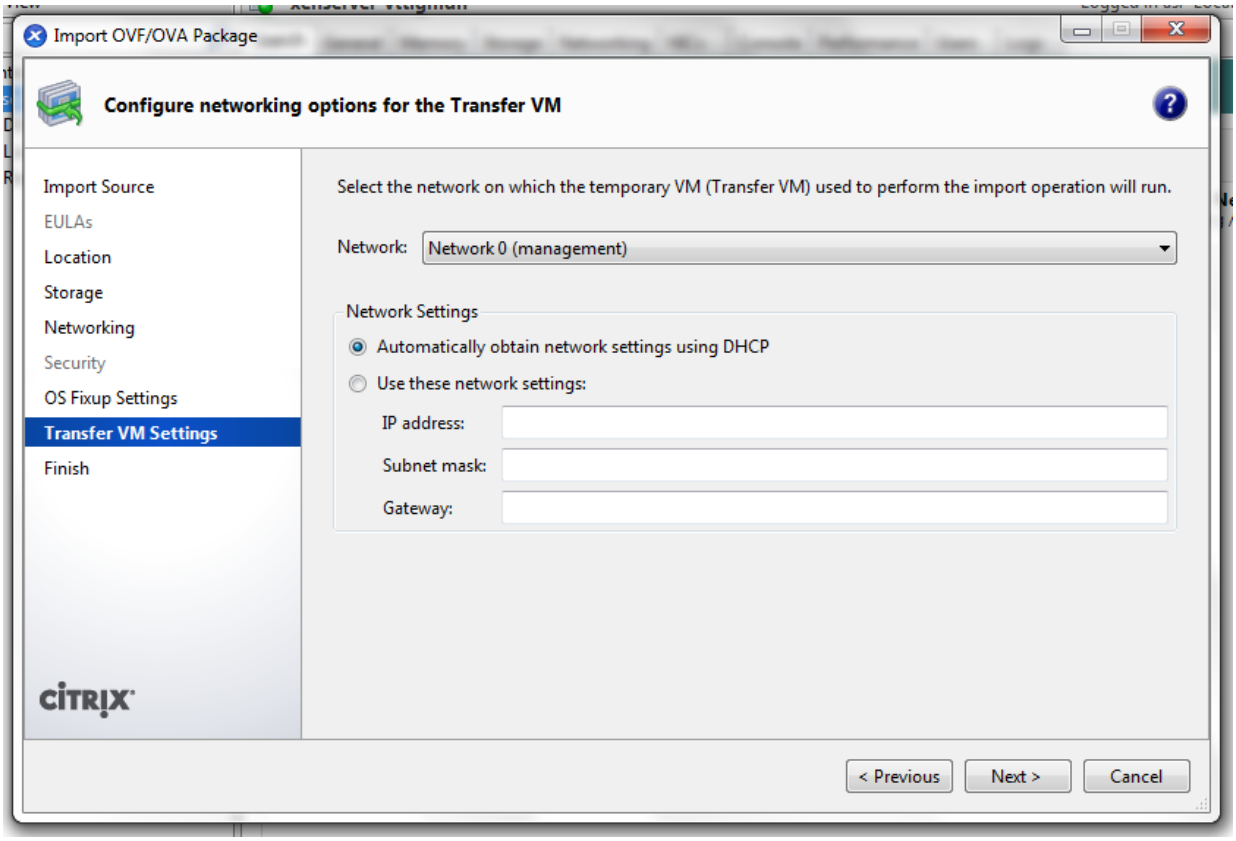
Alternatively, you can configure this after deployment but before startup. For details, see Mapping the virtual NICs (vNICs) to physical NICs on page 76.

If your FortiWeb-VM will be operating in transparent mode, you must configure the network mappings to match. See Configuring the vNetwork for the transparent modes on page 81.

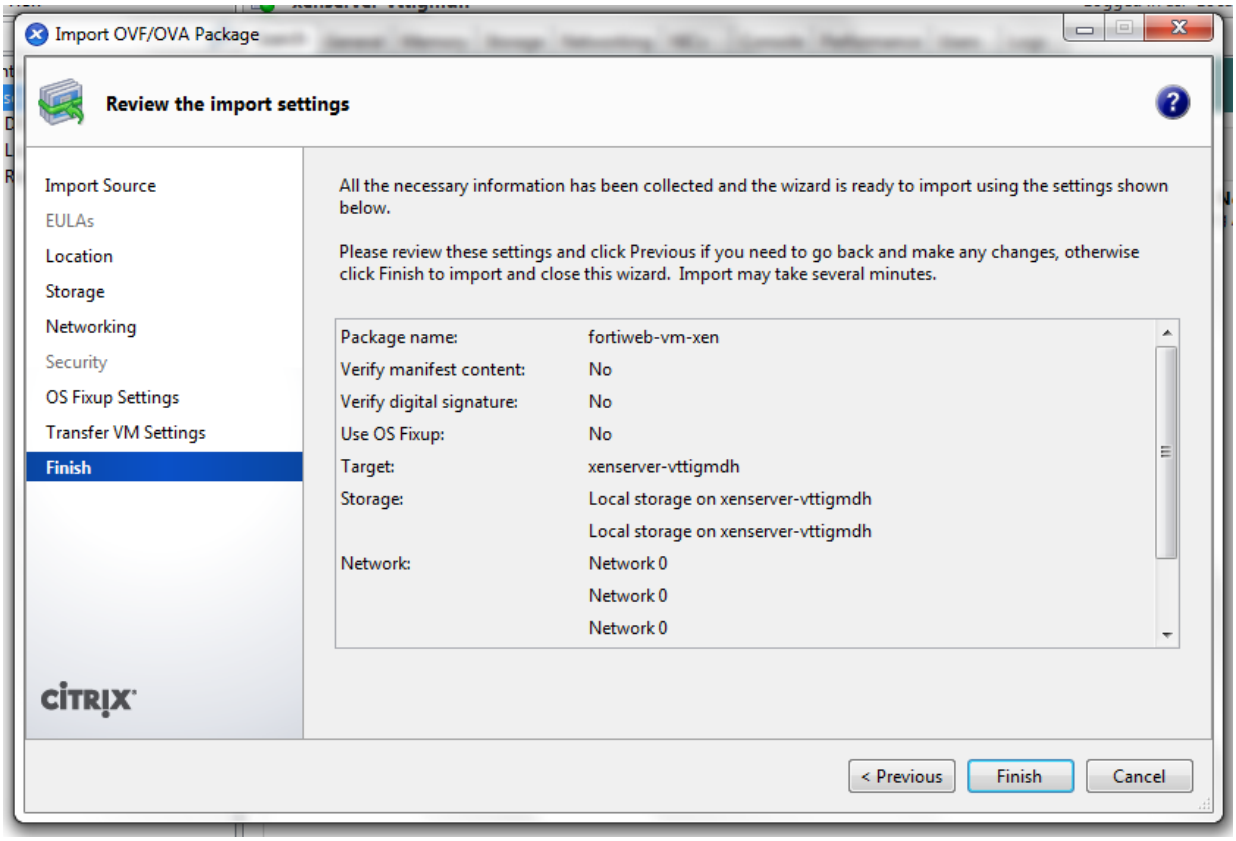
9. Click **Next** to skip OS fixup.



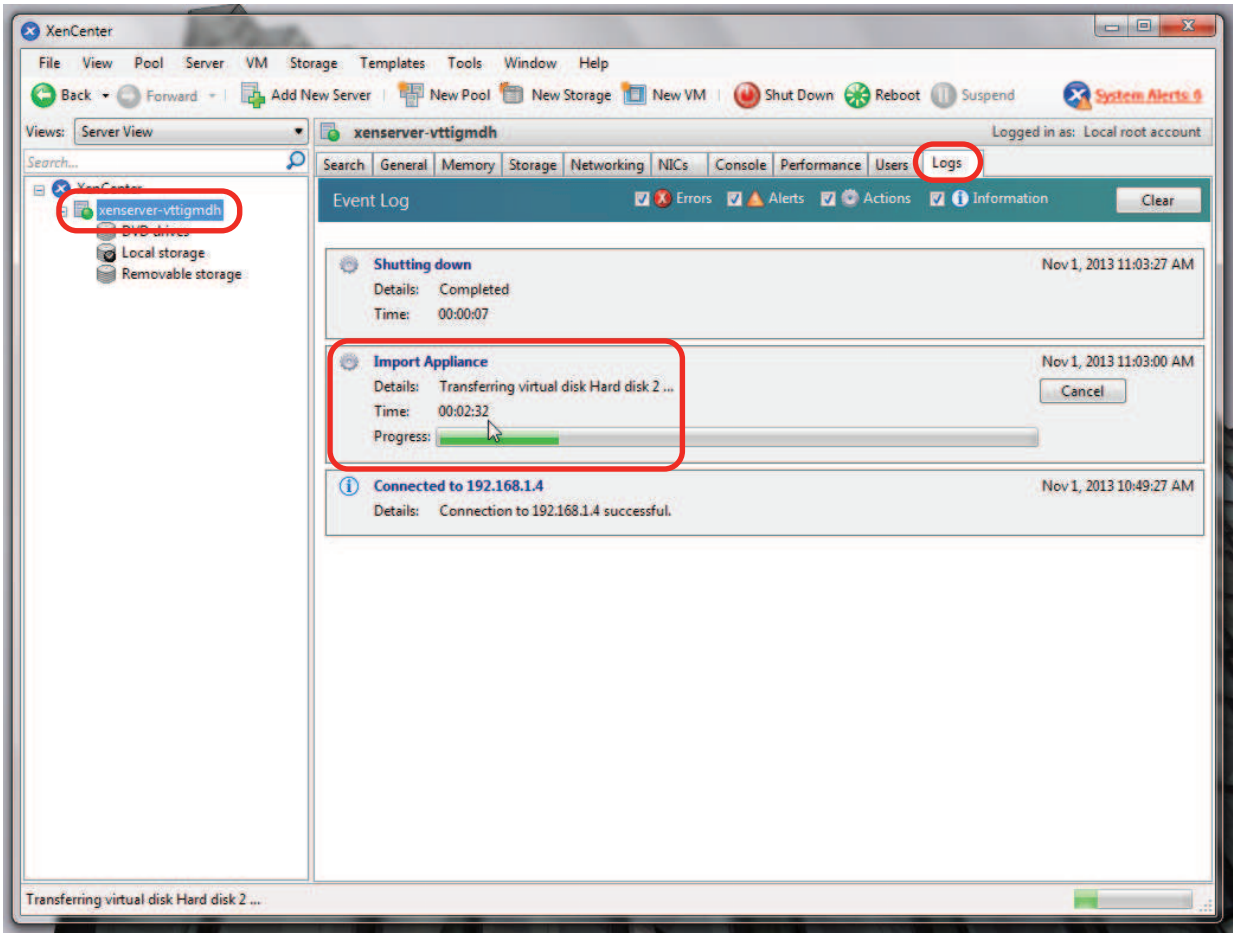
10. Configure temporary network settings that XenServer can use to download FortiWeb-VM, then click **Next**.



11. Click **Finish** to send the FortiWeb-VM image and its VM settings to XenServer.



The client connects to the VM environment, and deploys the image to it. Time required depends on your computer's hardware speed and resource load, and also on the file size and speed of the network connection, but might take 15 minutes to complete.



When complete, the deployment should appear in the list of deployed VMs for that XenServer, in the pane on the left side of XenCenter.

Continue with Configuring the virtual appliance's virtual hardware settings on page 67.

Do **not** power on the virtual appliance **until** you:

- Resize the virtual disk (VMDK) (see Resizing the virtual disk (vDisk) on page 67)
- Set the number of vCPUs (see Configuring the number of virtual CPUs (vCPUs) on page 70)
- Set the vRAM on the virtual appliance (Configuring the virtual RAM (vRAM) limit on page 73)
- Map the virtual network adapter(s) (Mapping the virtual NICs (vNICs) to physical NICs on page 76).

These settings cannot be configured inside FortiWeb-VM, and must be configured in the VM environment. **Some settings cannot be easily reconfigured after you power on the virtual appliance.**

Configuring the virtual appliance's virtual hardware settings

After installing FortiWeb-VM, log in to Citrix XenServer on the server and configure the virtual appliance's hardware settings to suit the size of your deployment. For sizing guidelines, contact your reseller or Fortinet Technical Support.

For information on the limits of configurable values for FortiWeb-VM, see the *FortiWeb Administration Guide*.

Resizing the virtual disk (vDisk)

If you configure the virtual appliance's storage repository to be internal (i.e. local, on its own vDisk), resize the vDisk **before** powering on.

This step is not applicable if the virtual appliance will use external network file system (such as NFS) datastores.

The FortiWeb-VM package that you downloaded includes pre-sized VMDK (Virtual Machine Disk Format) files. However, they are only 32 GB, which is not large enough for most deployments. **Resize the vDisk before powering on the virtual machine.**

Before doing so, make sure that you understand the effects of your vDisk settings.

For example, if you have an 800 GB data store which has been formatted with 1 MB block size, you cannot size a single vDisk greater than 256 GB on your FortiWeb-VM.

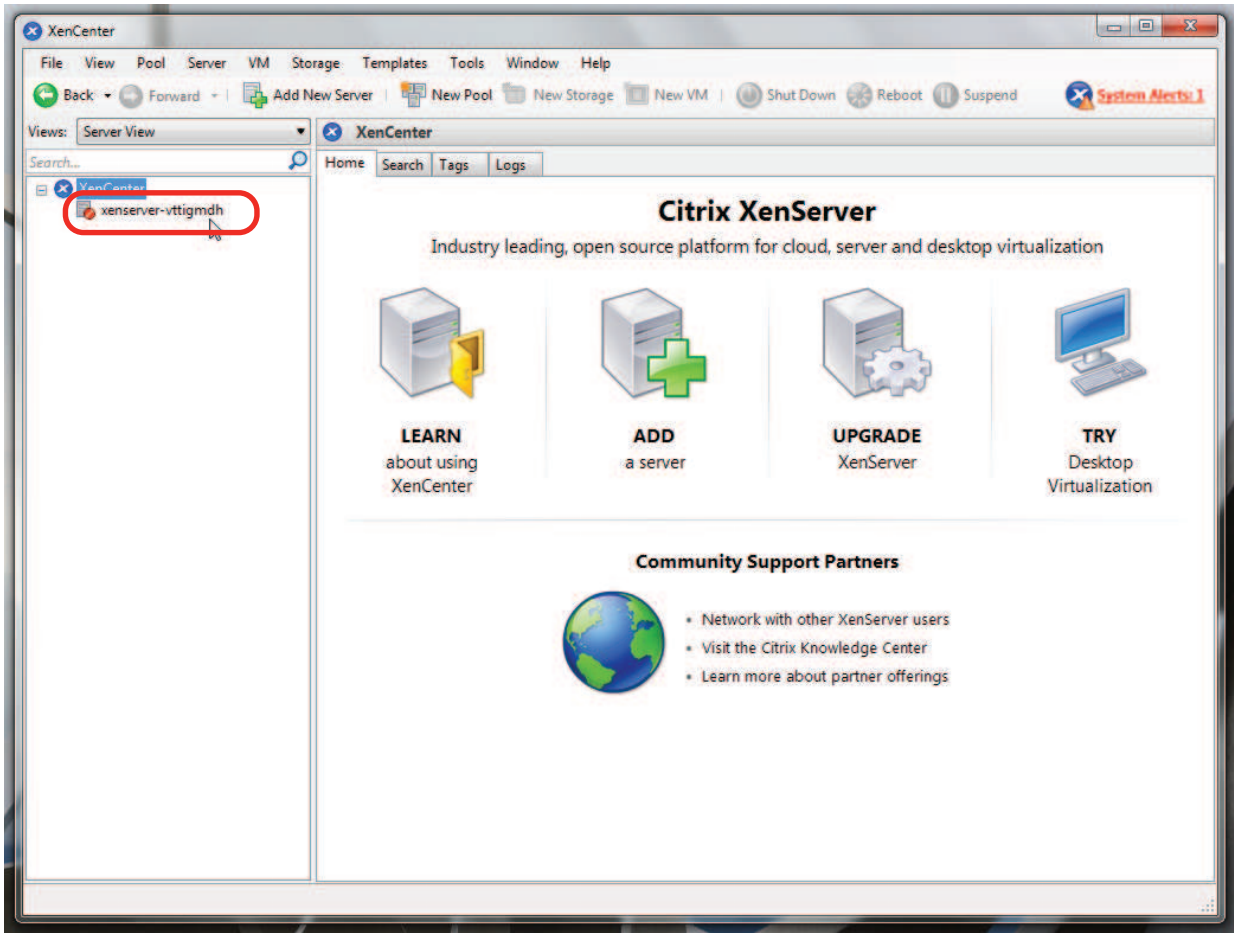
Consider also that, depending on the size of your organization's network, you might require more or less storage for your auto-learning data, anti-defacement backups, scan results, and reports.

To resize the vDisk

If you are resizing the disk for an existing deployment of FortiWeb-VM, back up the logs and other non-configuration data **before** beginning this procedure. **Formatting the disk will delete all data on that disk.** For backup instructions, see the *FortiWeb Administration Guide*.

While resizing the vDisk, the FortiWeb-VM must be powered off.

1. On your management computer, start Citrix XenCenter.

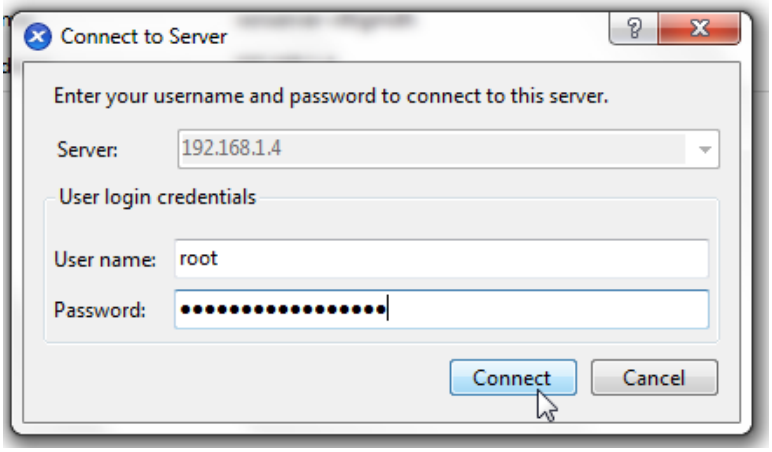


2. In the pane on the left side, double-click the name of the XenServer. This will open an authentication dialog.
3. In **Server**, type the IP address or FQDN of the Citrix XenServer server.

   In **User name**, type the name of your account on that server.

   In **Password**, type the password for your account on that server.

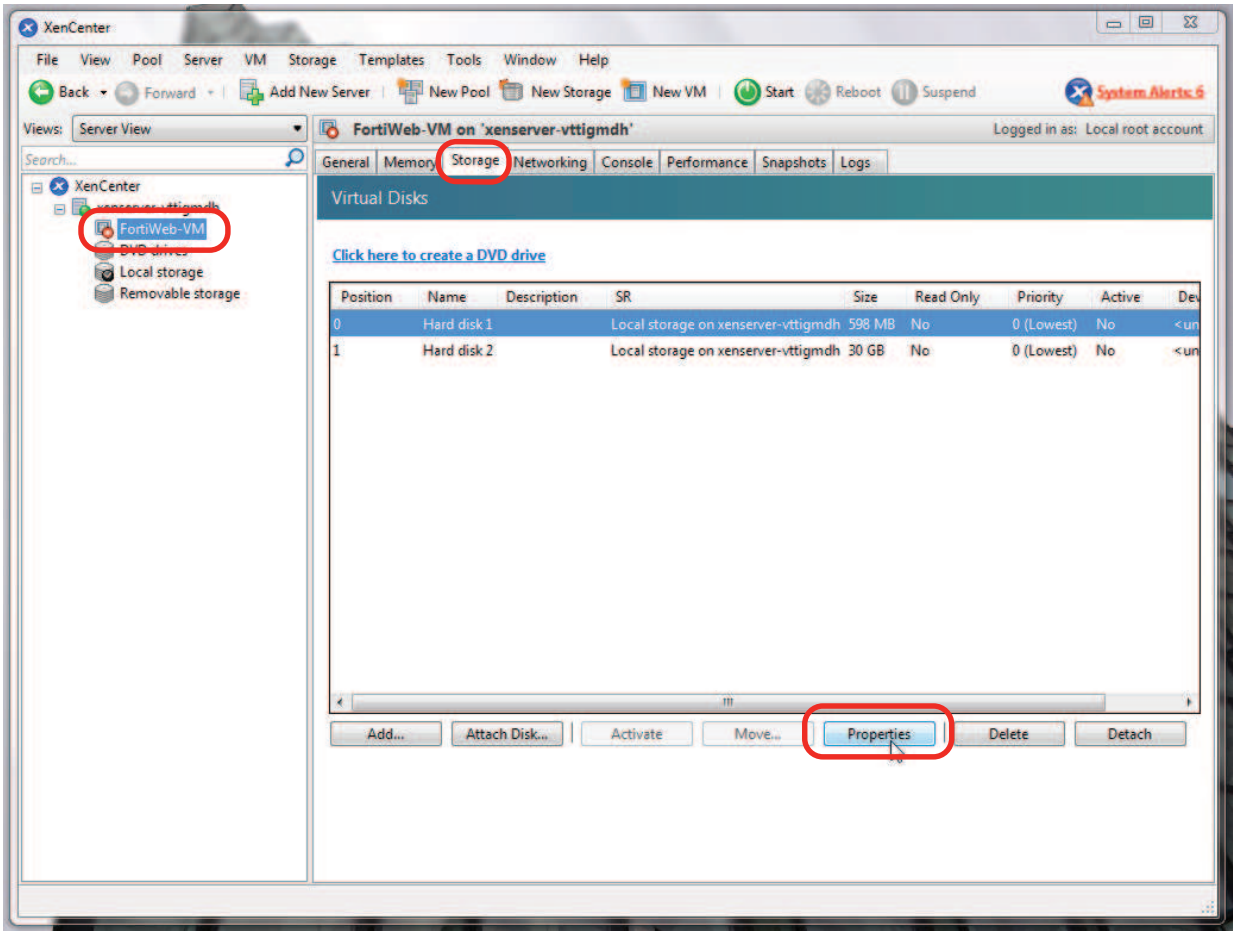
Click *Connect*.



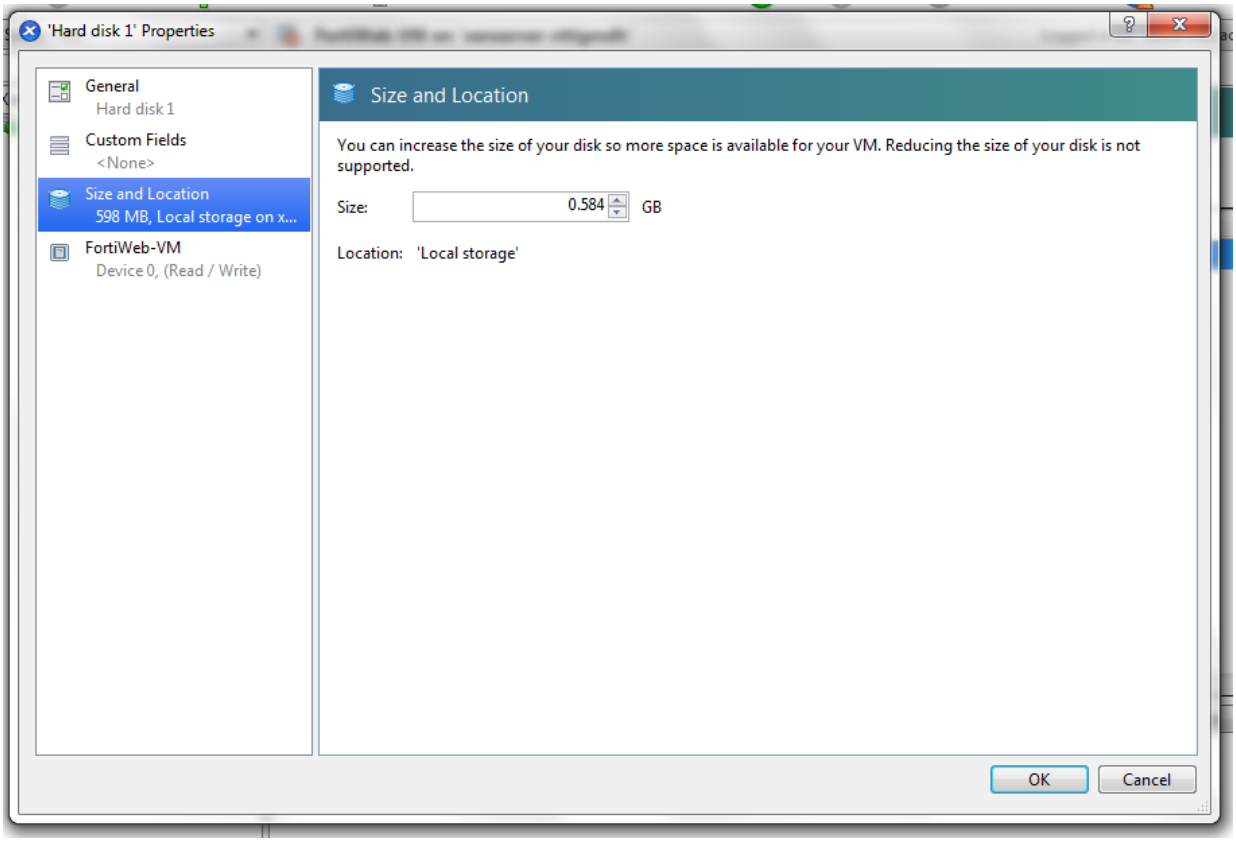
4. In the pane on the left side, select the name of the FortiWeb-VM instance on that server.

   The pane on the right side will change to show the settings for this specific virtual machine.

5. In the pane on the right side, click the **Storage** tab, then click the **Properties** button.



6. Adjust the maximum size of the vDisk, then click **OK**.



Configuring the number of virtual CPUs (vCPUs)

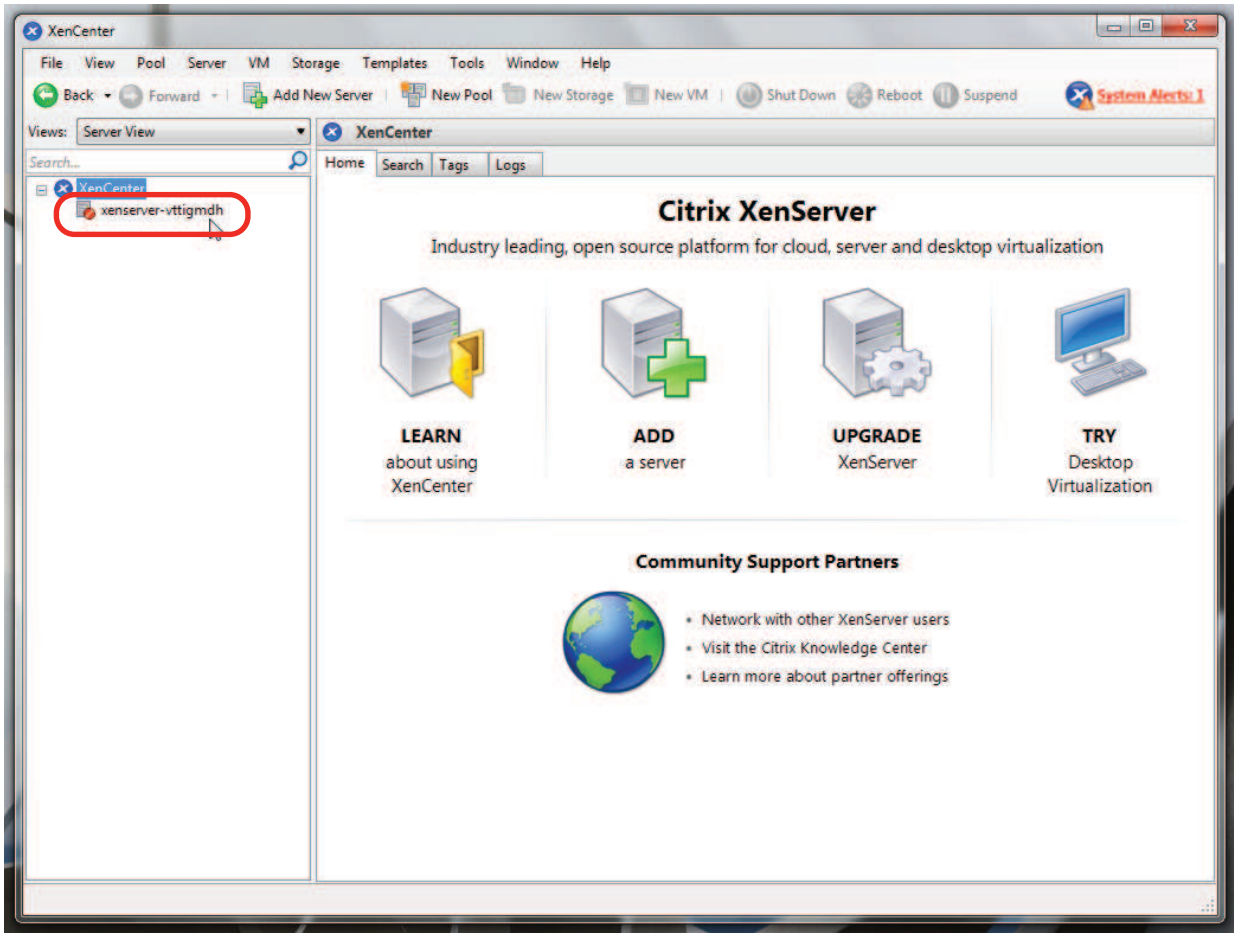
By default, the virtual appliance is configured to use 1 vCPU. Depending on the FortiWeb-VM license that you purchased, you can allocate up to 1, 2, 4, or 8 vCPUs.

If you need to increase or decrease the vCPUs after the initial boot, power off FortiWeb-VM, adjust the number of vCPUs, then see Updating the license for more vCPUs on page 155.

To change the number of vCPUs

While resizing the vCPU, the FortiWeb-VM must be powered off.

1. On your management computer, start Citrix XenCenter.

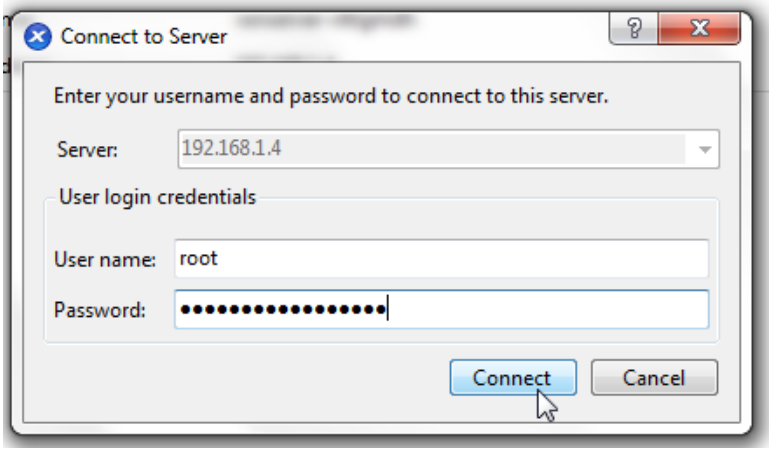


2. In the pane on the left side, double-click the name of the XenServer. This will open an authentication dialog.
3. In **Server**, type the IP address or FQDN of the Citrix XenServer server.

   In **User name**, type the name of your account on that server.

   In **Password**, type the password for your account on that server.

Click *Connect*.



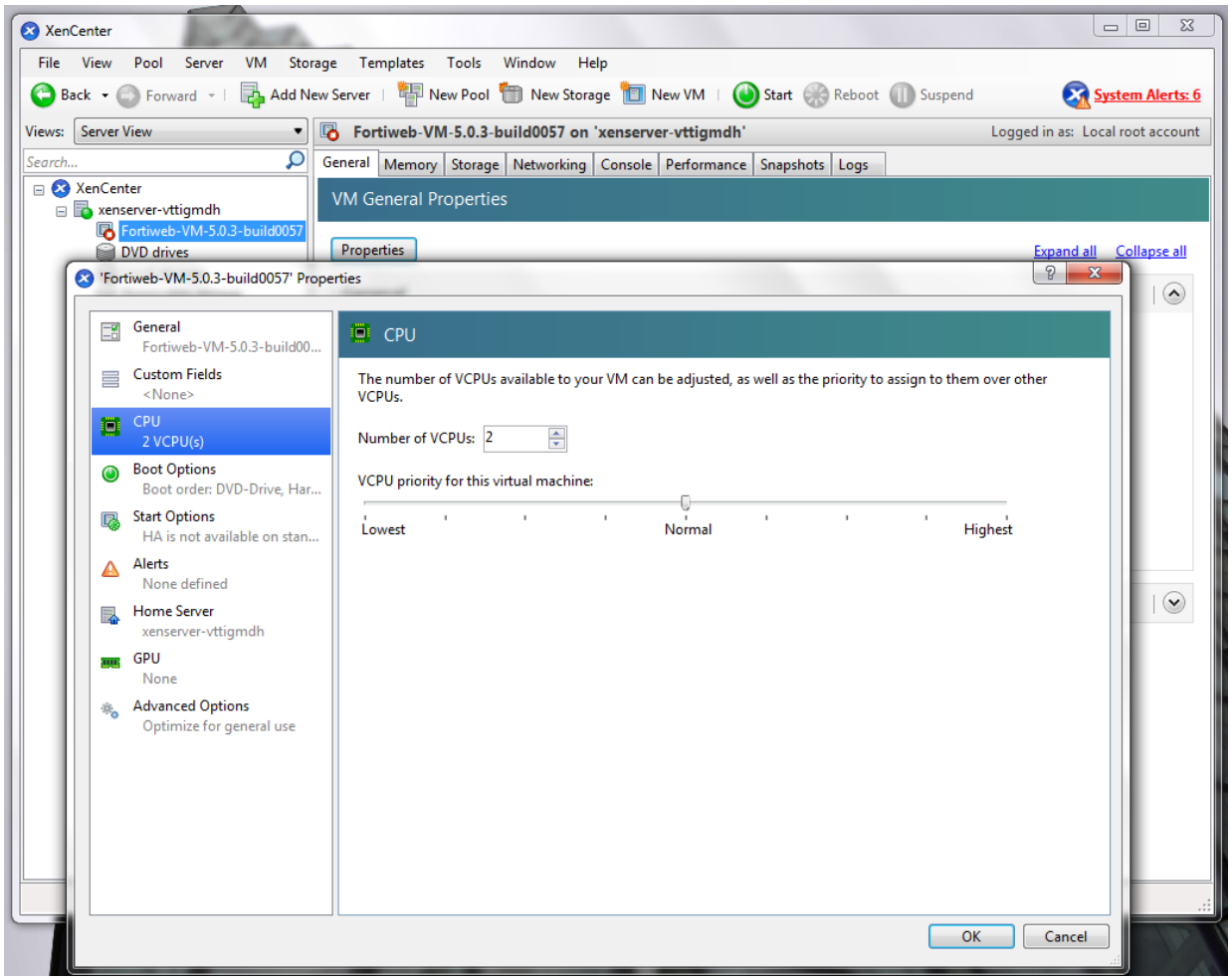
4. In the pane on the left side, select the name of the FortiWeb-VM instance.

   The pane on the right side will change to show the settings for this specific virtual machine.

5. In the pane on the right side, click **Properties**.

   The virtual appliance's properties dialog appears.

6. In *Number of VCPUs*, type the maximum number of vCPUs to allocate. Valid values range from 1 to 8.



7. Click *OK*.
8. If you do not need to change the other resources, continue with Powering on the virtual appliance on page 86. Otherwise continue with Configuring the virtual RAM (vRAM) limit on page 73.

Configuring the virtual RAM (vRAM) limit

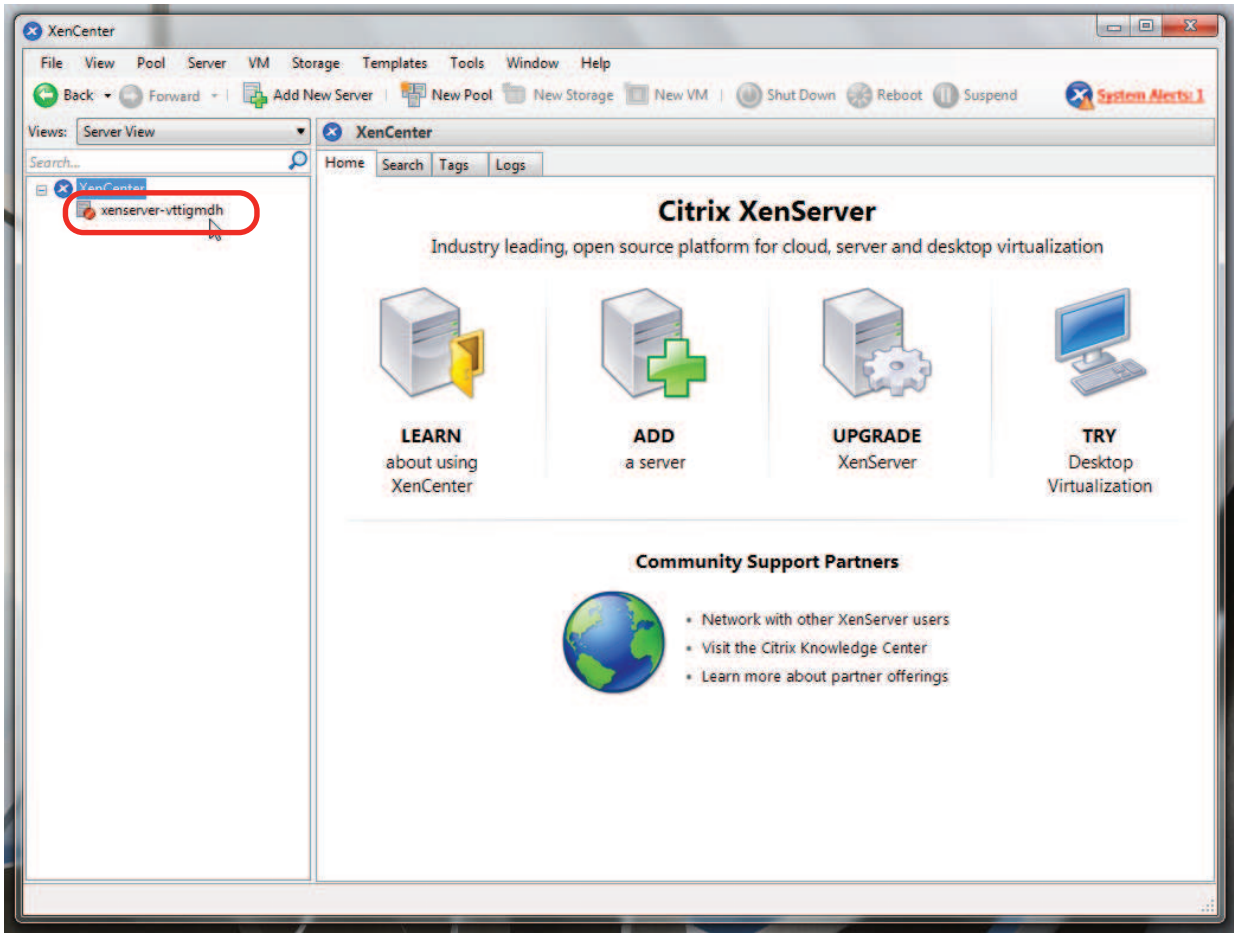
FortiWeb-VM comes pre-configured to use 4 GB of vRAM. You can change this value.

It is possible to configure FortiWeb-VM to use less vRAM, such as 2 GB. However, for performance reasons, it is not recommended.

To change the amount of vRAM

While resizing the vRAM, the FortiWeb-VM must be powered off.

1. On your management computer, start Citrix XenCenter.

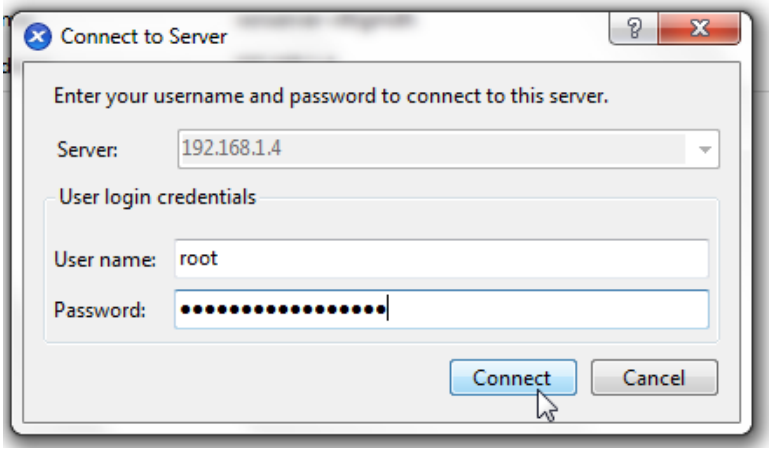


2. In the pane on the left side, double-click the name of the XenServer. This will open an authentication dialog.
3. In **Server**, type the IP address or FQDN of the Citrix XenServer server.

   In **User name**, type the name of your account on that server.

   In **Password**, type the password for your account on that server.

Click *Connect*.



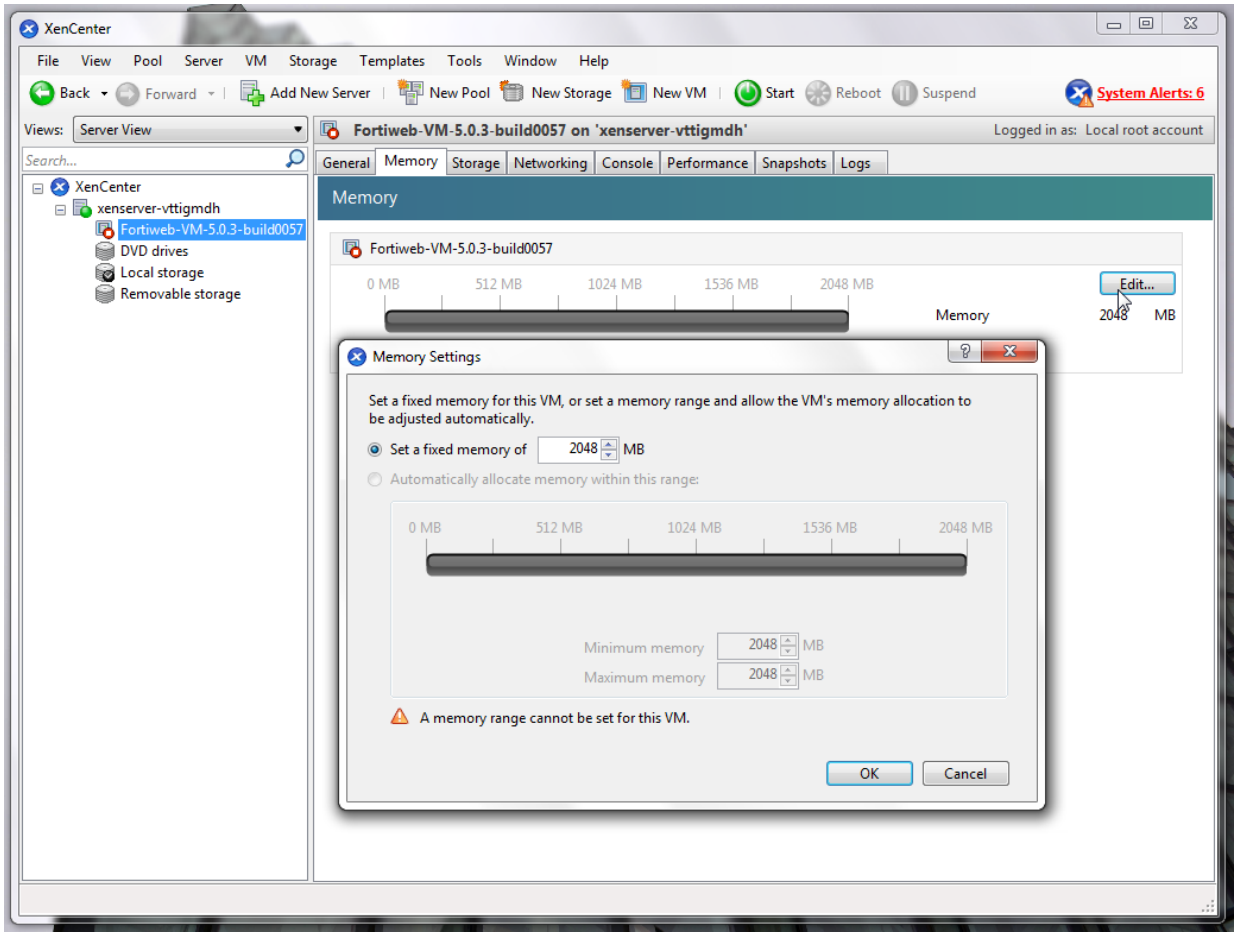
4. In the pane on the left side, select the name of the FortiWeb-VM instance on that server.

   The pane on the right side will change to show the settings for this specific virtual machine.

5. In the pane on the right side, click the **Memory** tab, then click **Edit**.

   The virtual appliance's memory settings dialog appears.

6. Adjust the maximum amount in gigabytes (GB) of the vRAM to allocate, then click **OK**.



7. If you do not need to change the other resources, continue with Powering on the virtual appliance on page 86. Otherwise continue with Mapping the virtual NICs (vNICs) to physical NICs on page 76.

Mapping the virtual NICs (vNICs) to physical NICs

Appropriate mappings of the FortiWeb-VM network adapter ports to the host computer's physical ports depends on your existing virtual environment.

Often, the default bridging vNICs work, and don't need to be changed.

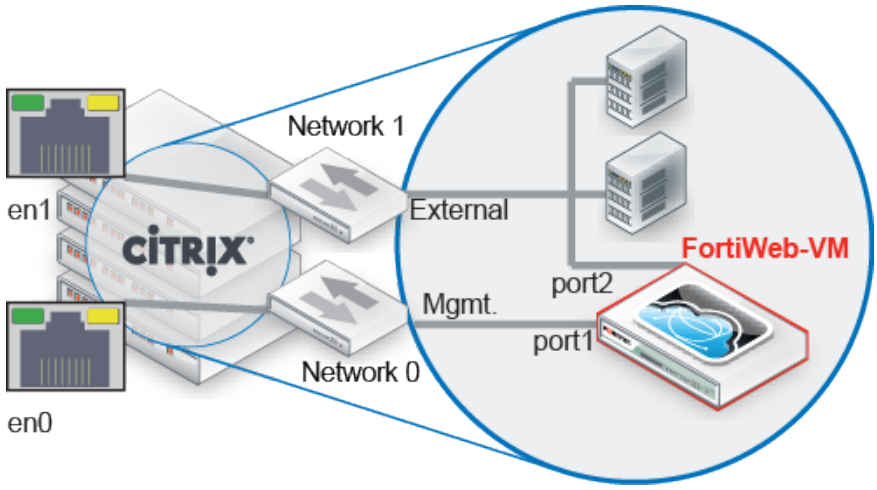
If you are unsure of your network mappings, try bridging first **before** non-default vNIC modes such as NAT or host-only networks. The default bridging vNIC mappings are appropriate where each of the host's guest virtual machines should have their own IP addresses on your network.

The most common exceptions to this rule are for VLANs and the transparent modes. See Configuring the vNetwork for the transparent modes on page 40.

When you deploy the FortiWeb-VM package, 4 bridging vNICs are created and automatically mapped to a port group on 1 virtual switch (vSwitch) within the hypervisor. Each of those vNICs can be used by one of the 4 network interfaces in FortiWeb-VM. (Alternatively, if you prefer, some or all of the network interfaces may be configured to use the same vNIC.) vSwitches are themselves mapped to physical ports on the server.

You can change the mapping, or map other vNICs, if either your VM environment requires it or the FortiWeb-VM will be operating in either true transparent proxy or transparent inspection mode. (For information on how to choose the operation mode, see the setup instructions in the *FortiWeb Administration Guide*.)

The following table provides an example of how vNICs could be mapped to the physical network ports on a server.

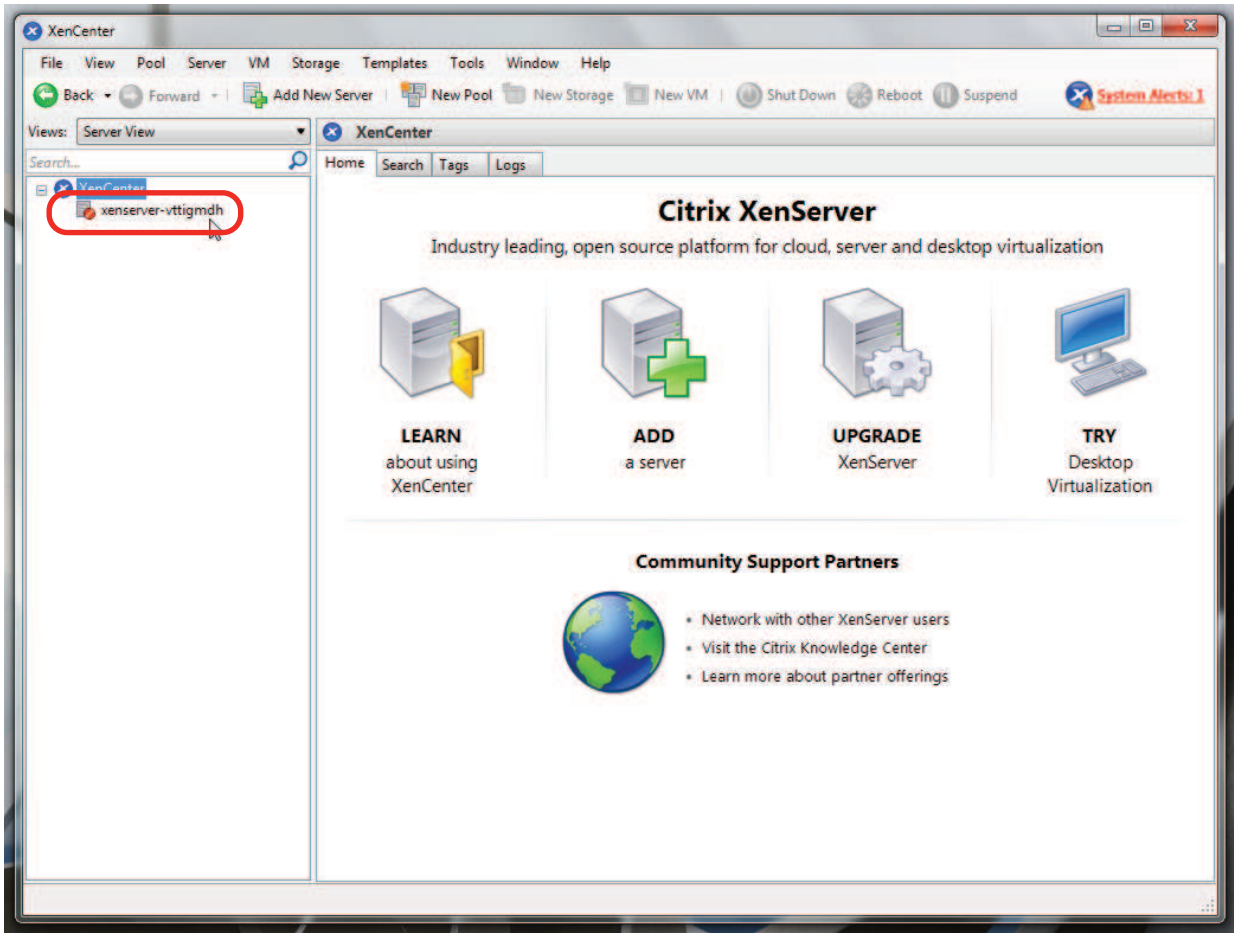


Example: Network mapping for reverse proxy mode

Citrix XenServer			FortiWeb-VM
Physical Network Adapter	**Network Mapping (vSwitch Port Group)**	**Virtual Network Adapter for FortiWeb-VM**	**Network Interface Name in Web UI/CLI**
eth0	Network 0	Management	port1
		External	port2
eth1		Internal	port3
	Network 1	External	port4

To map network adapters

1. On your management computer, start Citrix XenCenter.

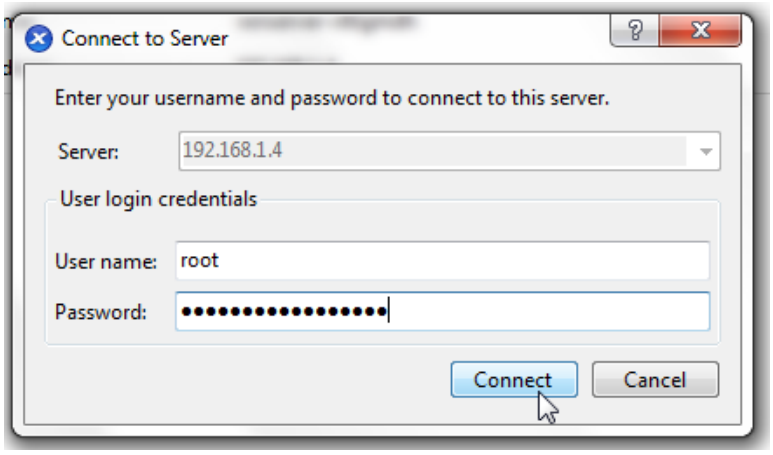


2. In the pane on the left side, double-click the name of the XenServer. This will open an authentication dialog.
3. In **Server**, type the IP address or FQDN of the Citrix XenServer server.

   In **User name**, type the name of your account on that server.

   In **Password**, type the password for your account on that server.

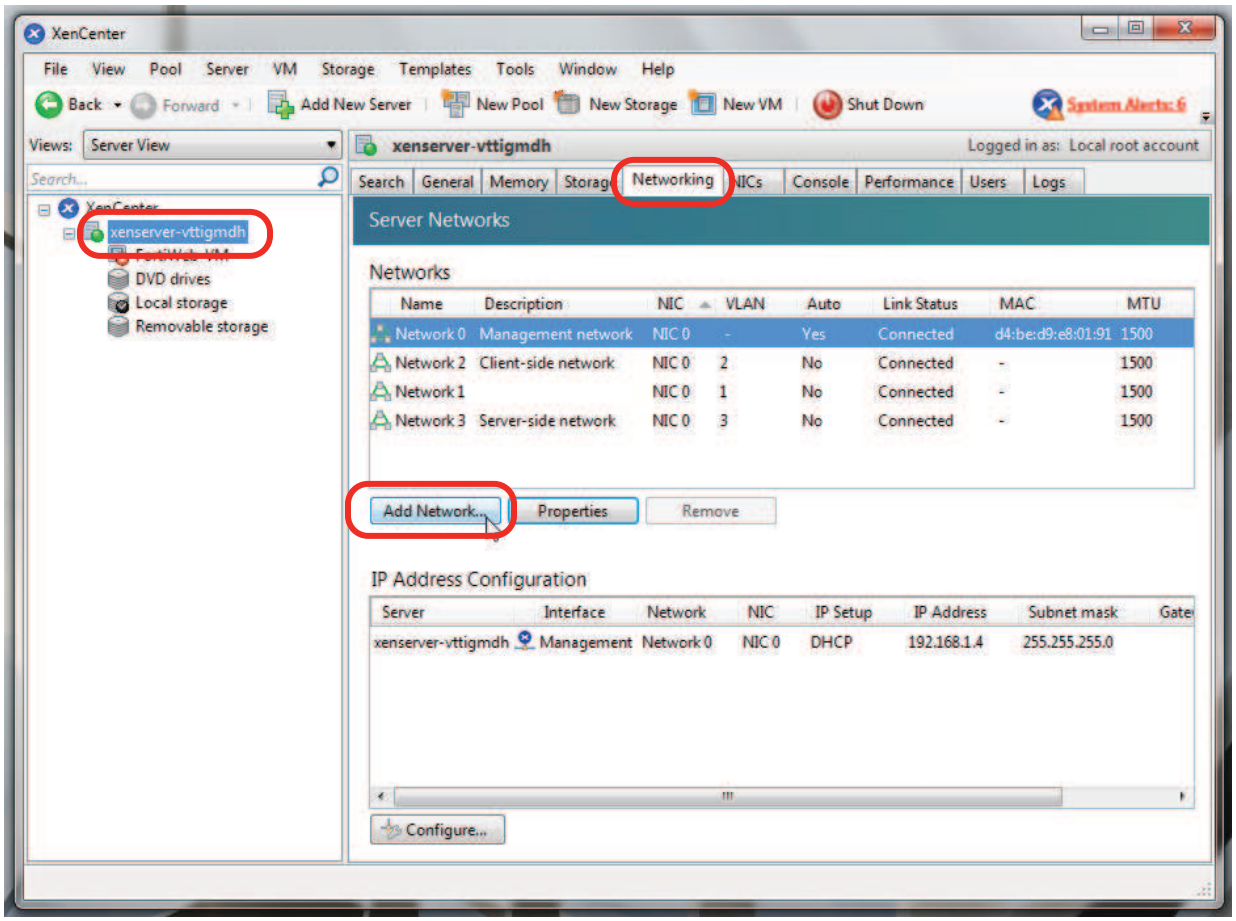
   Click **Connect**.



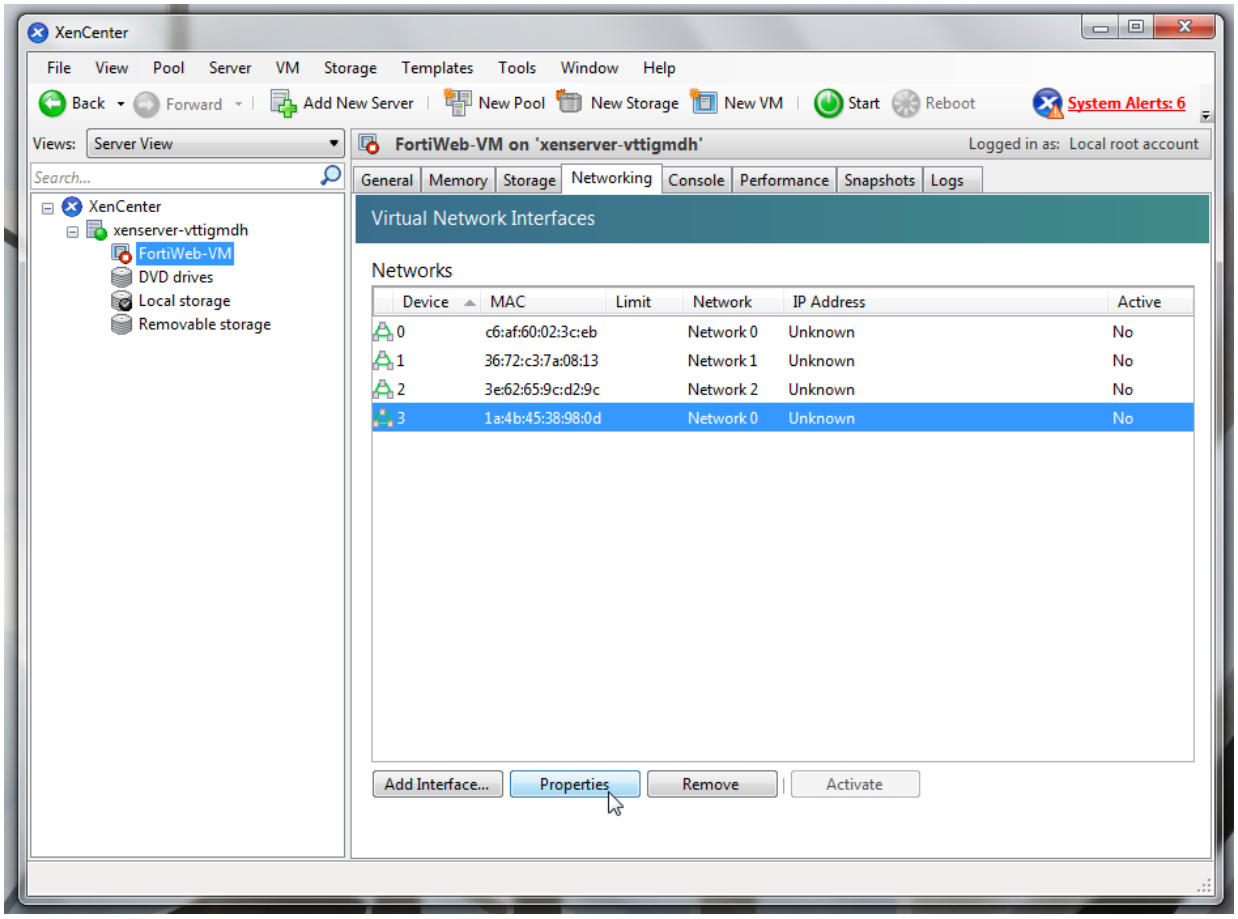
4. In the pane on the right side, click the **Networking** tab, then click **Add Network**.

   The hypervisor's networking dialog appears.

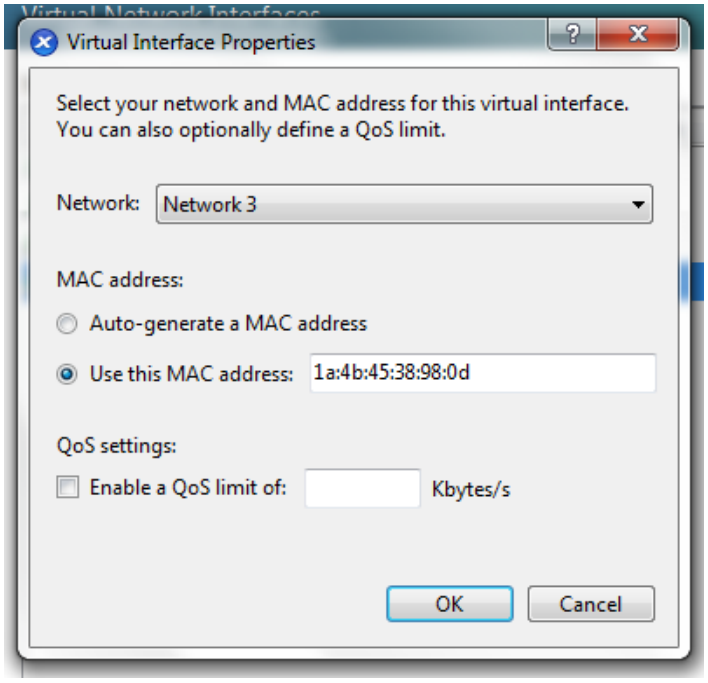
5. In the list of virtual hardware on the left side of the dialog, click the name of a virtual network adapter to see its current settings.



6. From the **Network Connection** drop-down menu, select the virtual network mapping for the virtual network adapter.



The correct mapping varies by your virtual environment's network configuration. In the example illustration below, the vNIC is mapped to the virtual network (vNetwork) named **Network 3.**



7. Click **OK**.
8. Continue with Powering on and shutting down the virtual appliance on page 45.

Configuring the vNetwork for the transparent modes

The default vNetwork configuration does **not** function with FortiWeb bridges (V-zones). You use bridges when you deploy your FortiWeb-VM in either true transparent proxy or transparent inspection operation mode.

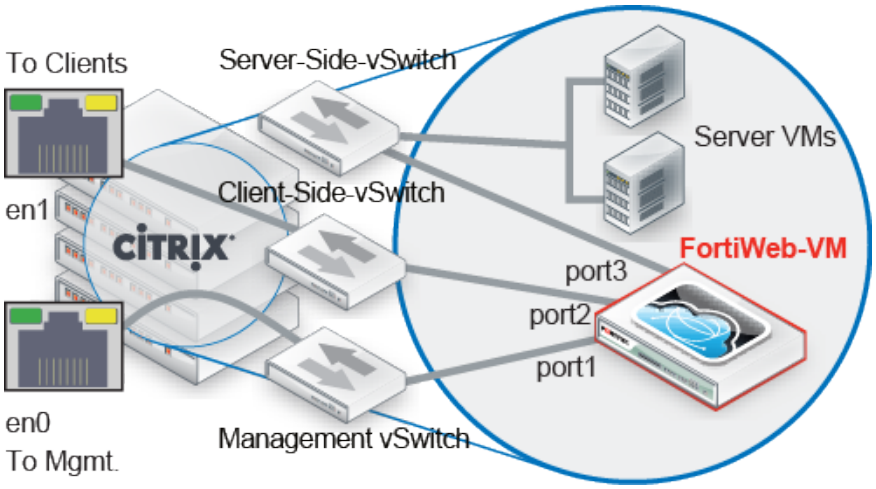
Use the following general configuration steps to support the transparent modes:

- Add 2 vSwitches or distributed vSwitches (dvSwitch) for the bridge: one for the web server side, and one for the client side

  Alternatively, add a single vSwitch that provides two different VLAN IDs. Use these IDs to create VLAN subinterfaces to add to a bridge.

- Set both to promiscuous mode
- Set each vSwitch you add to promiscuous mode and map it to a network adapter (vNIC)

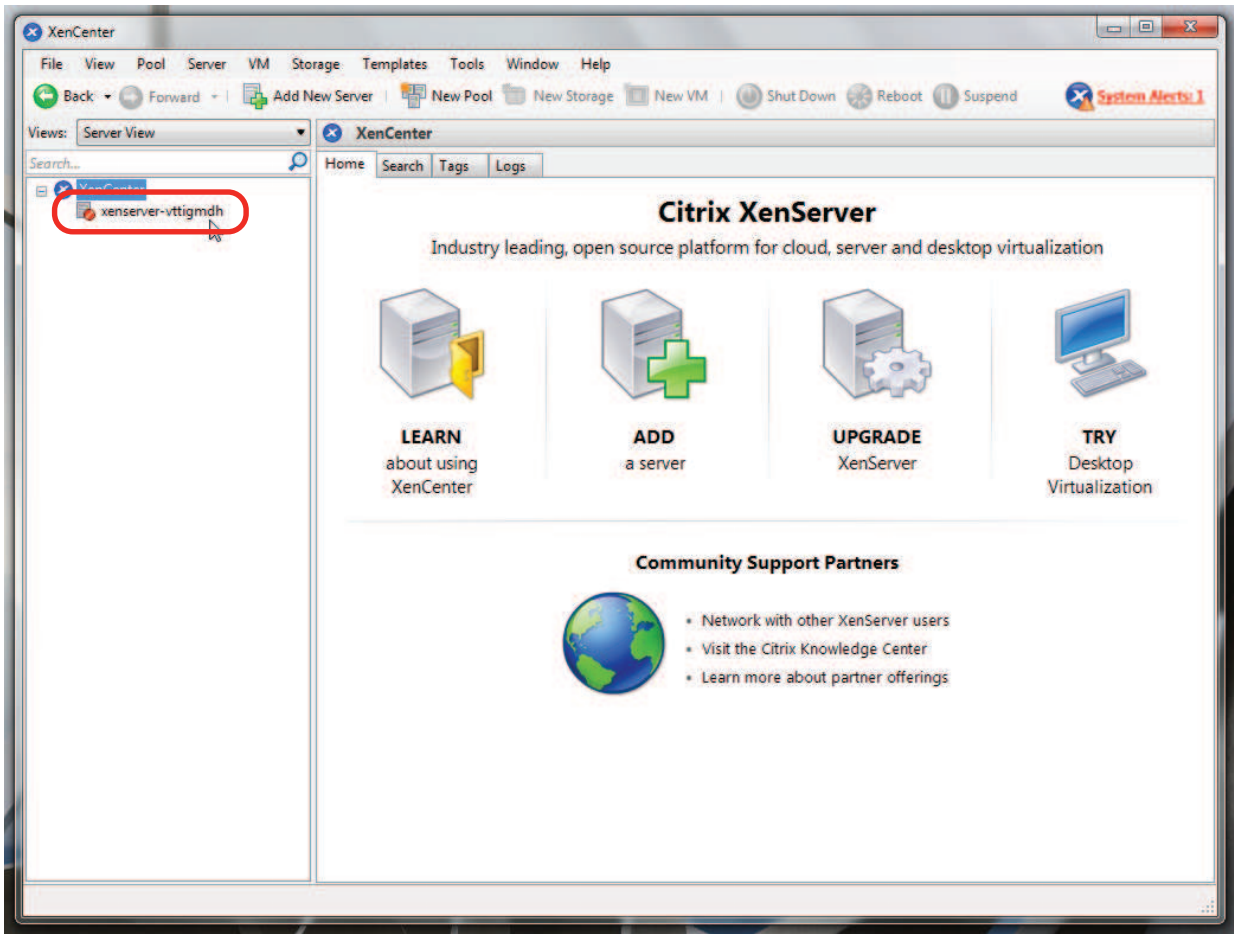
Similar to a deployment that does not use virtual machines, connections between clients and servers travel through the two vSwitches (or two VLANs) that comprise the bridge, with FortiWeb-VM in between them.



The following instructions assume your configuration uses 2 vSwitches.

To create a vSwitch

1. On your management computer, start Citrix XenCenter.



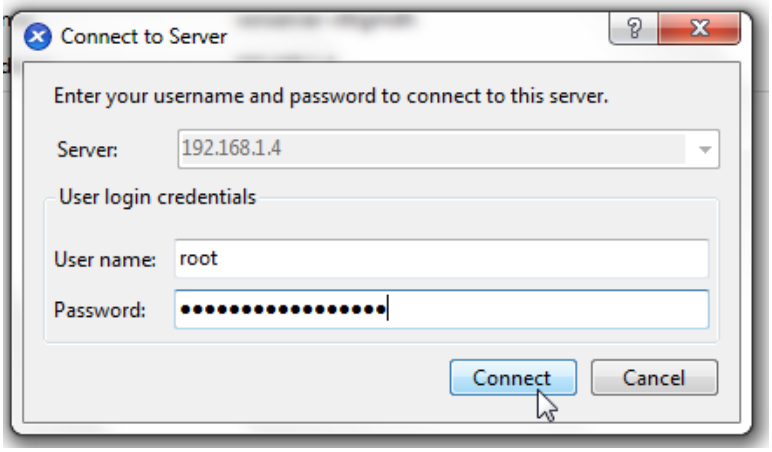
2. In the pane on the left side, double-click the name of the XenServer. This will open an authentication dialog.

3. In **Server**, type the IP address or FQDN of the Citrix XenServer server.

   In **User name**, type the name of your account on that server.

   In **Password**, type the password for your account on that server.

   Click **Connect**.

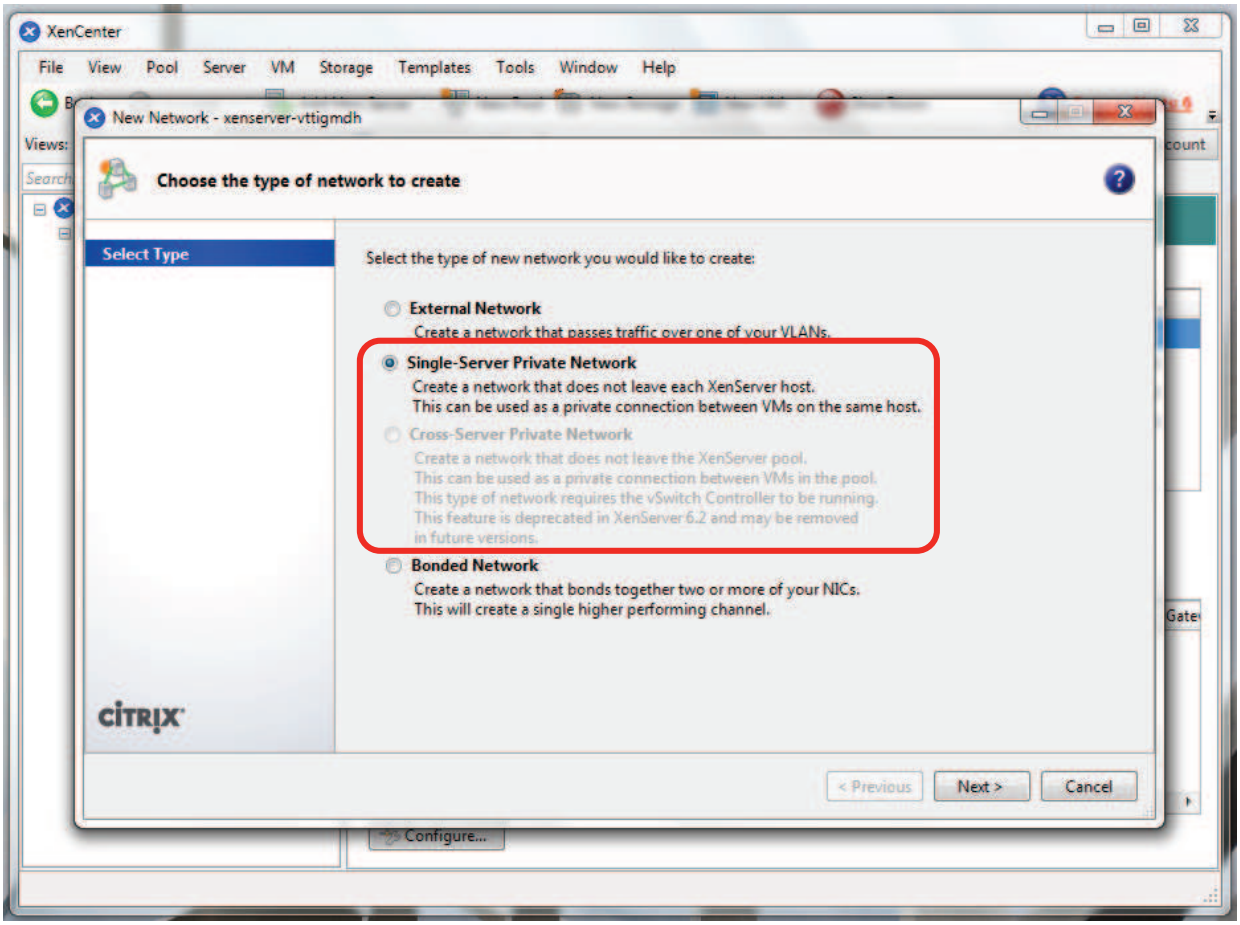


4. In the pane on the left side, select either the name of a XenServer pool, or (if your web servers are on the same XenServer as FortiWeb-VM) a single XenServer.

   vSwitches will allow communication between different Xen Servers in the same pool.

5. On the **Configuration** tab, click **Networking**.

   A window appears where you can configure single server vSwitches or (if you selected a pool in the previous step) distributed vSwitches.



6. Depending on whether FortiWeb-VM will run transparently between clients and web servers on the same Xen server, select either:

   - **Cross-Server Private Network** — Select this option if your web servers are **not** hosted on the same Xen server as your FortiWeb-VM, but are in the same resource pool.

     This option is greyed out and unavailable if you have not yet installed Citrix's Distributed Virtual Switch Controller (Open vSwitch) or have software-defined networking (SDN) available. You must also add the XenServer to the dvSwitch; enter this command on the CLI of each XenServer, then reboot it:

     ```
     xe-switch-network-backend openvswitch
     ```

   - **Single Server Private Network** — If your web servers are on the same Xen server as your FortiWeb-VM, you can select this option.

7. Click **Next**.
8. Follow the wizard, providing a name such as `Client-Side-vSwitch1` that identifies the port group.
9. Click **Finish**.
10. Repeat this procedure to create the other, server-side vSwitch.
11. Continue with To configure promiscuous mode for the new vSwitches.

To configure promiscuous mode for the new vSwitches

1. Connect to the CLI of the XenServer where you are deploying FortiWeb-VM.
2. To show the UUID of the vNetwork enter the command:

   ```
   xe pif-list network-name-label="Client-Side-vSwitch1"
   ```

   where `Client-Side-vSwitch1` is the name of a network as it appears in XenCenter.
3. Enter the command:

   ```
   xe pif-param-set uuid="0" other-config:promiscuous="true"
   ```

   where `0` is the UUID of the physical interface. If successful, the output of this command will verify that the physical interface is now in promiscuous mode:

   ```
   xe pif-param-list uuid="0"
   ```
4. To show the UUID of the virtual network interface, enter the command:

   ```
   xe vif-list vm-name-label=fortiweb-vm
   ```

   where `fortiweb-vm` is the name of the virtual machine as it appears in XenCenter.
5. Enter the command:

   ```
   xe vif-param-set uuid="0" other-config:promiscuous="true"
   ```

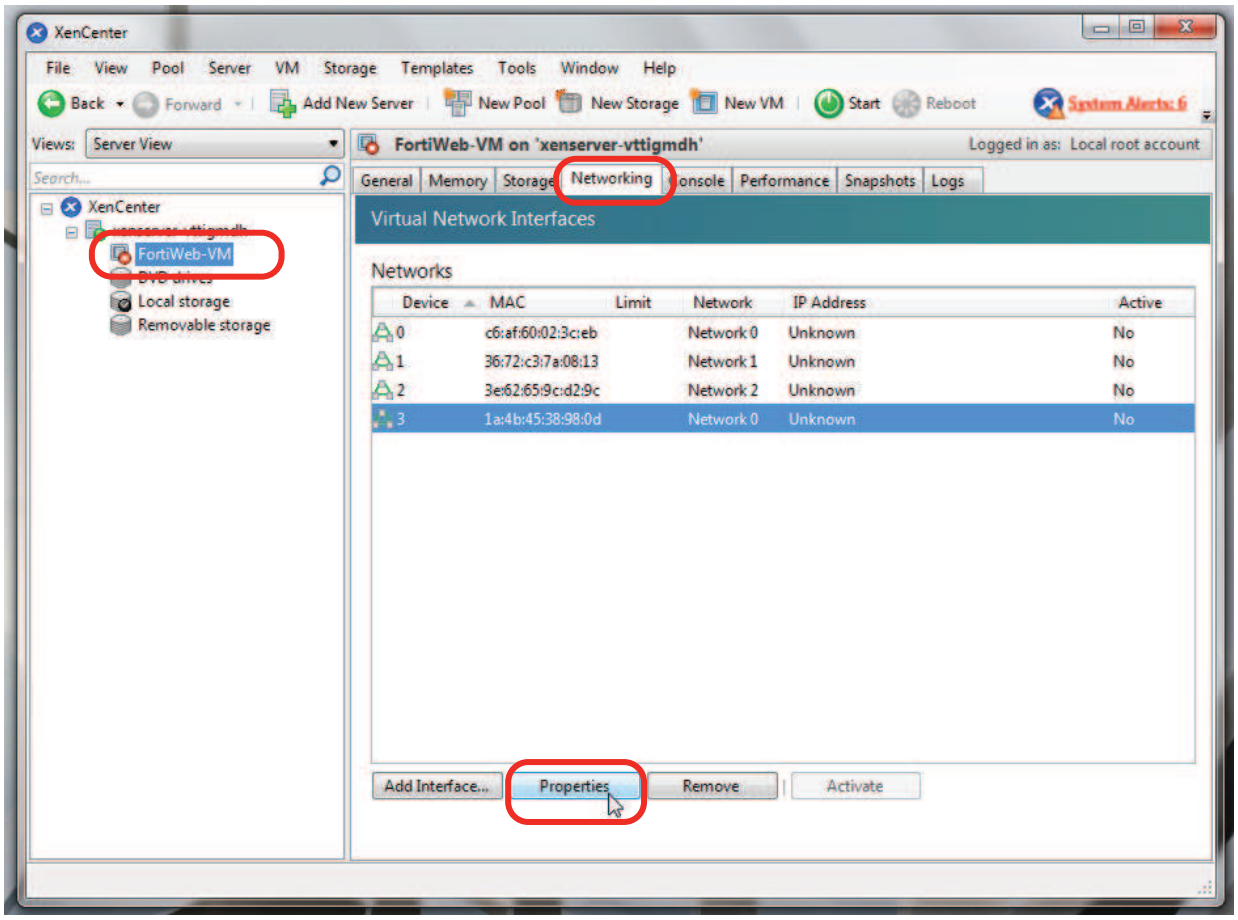
   where `0` is the UUID of the virtual interface. If successful, the output of this command will verify that the virtual interface is now in promiscuous mode:

   ```
   xe vif-param-list uuid="0"
   ```
6. Unplug and re-connect the virtual network interface by entering these commands:

   ```
   xe vif-unplug uuid="0"
   xe vif-plug uuid="0"
   ```
7. Repeat this procedure to configure the mode of the other, server-side vSwitch.
8. Continue with To map a network adapter to the new vSwitches.

To map a network adapter to the new vSwitches

1. In the pane on the left side, click the name of the virtual appliance, such as **FortiWeb-VM**.



2. On the **Networking** tab, select a vNIC (**Device**), then click **Properties.**

   A properties window appears.

3. Select the new vSwitch from the **Network** drop-down list.
4. Click **OK**.
5. Repeat this procedure with the other vSwitch for the bridge.
6. Later, when configuring FortiWeb-VM, add port2 and port3, or whichever FortiWeb ports correspond to the vSwitches you created in this procedure, to the bridge (V-zone).

Powering on the virtual appliance

Once the virtual appliance's package has been deployed and its virtual hardware configured, you can power on the virtual appliance.

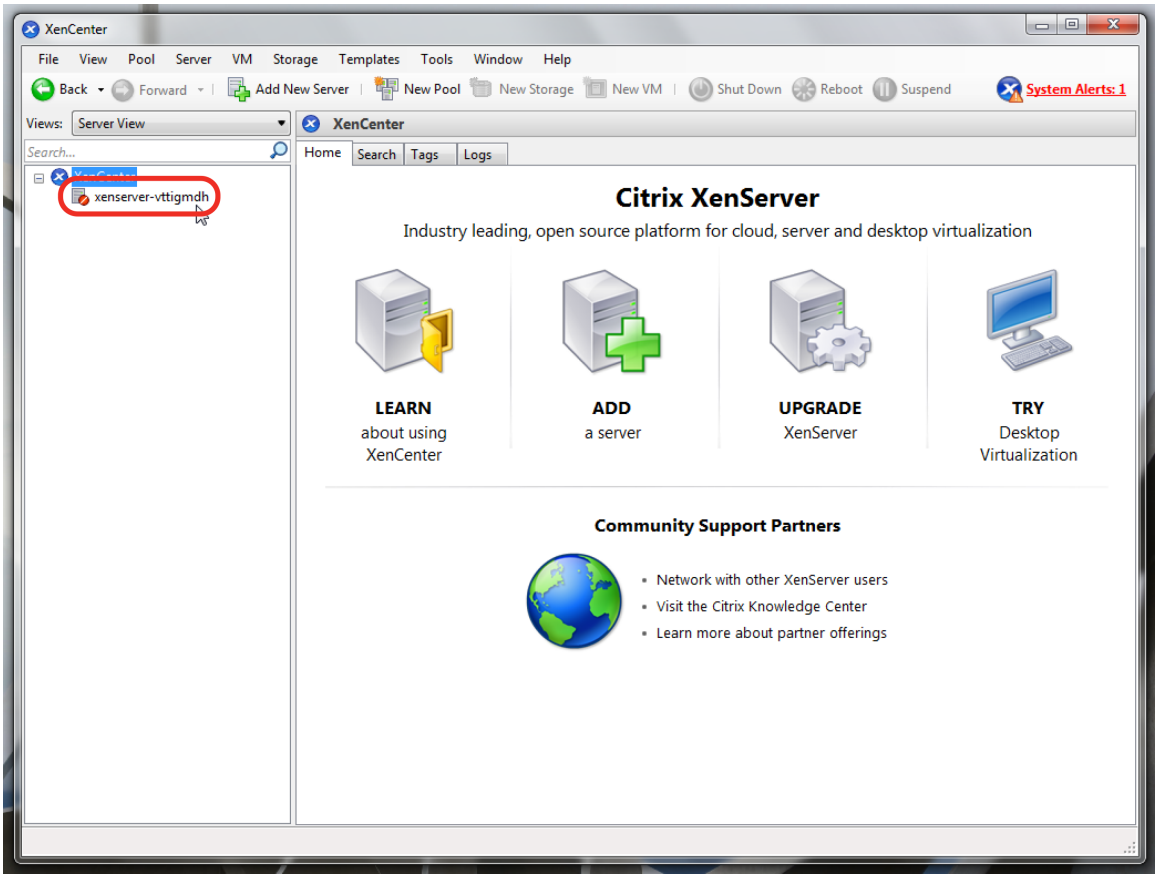
Do **not** power on the virtual appliance **unless** you have already mapped the virtual network adapter(s) (Mapping the virtual NICs (vNICs) to physical NICs on page 76). You may also want to:

- Resize disk (VMDK) (see Resizing the virtual disk (vDisk) on page 67)
- Configure the number of CPUs (see Configuring the number of virtual CPUs (vCPUs) on page 70)
- Set the RAM on virtual appliance (Configuring the virtual RAM (vRAM) limit on page 73)

These settings cannot be configured inside FortiWeb-VM, and must be configured in the virtual machine environment.

To power on FortiWeb-VM

1. On your management computer, start Citrix XenCenter.

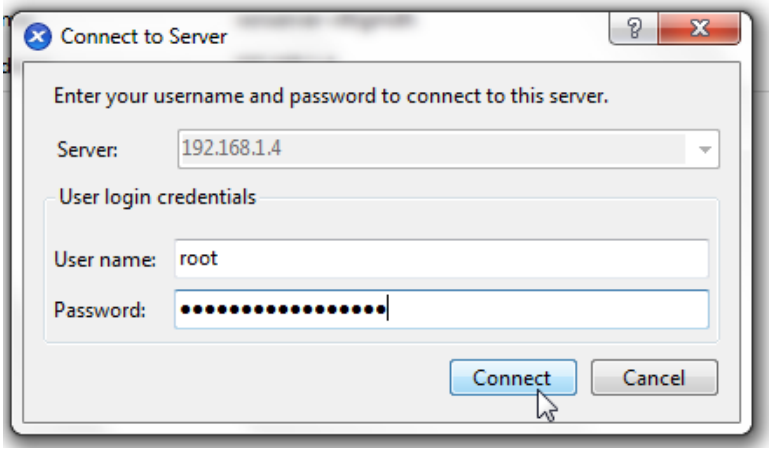


2. In the pane on the left side, double-click the name of the XenServer. This will open an authentication dialog.
3. In **Server**, type the IP address or FQDN of the Citrix XenServer server.

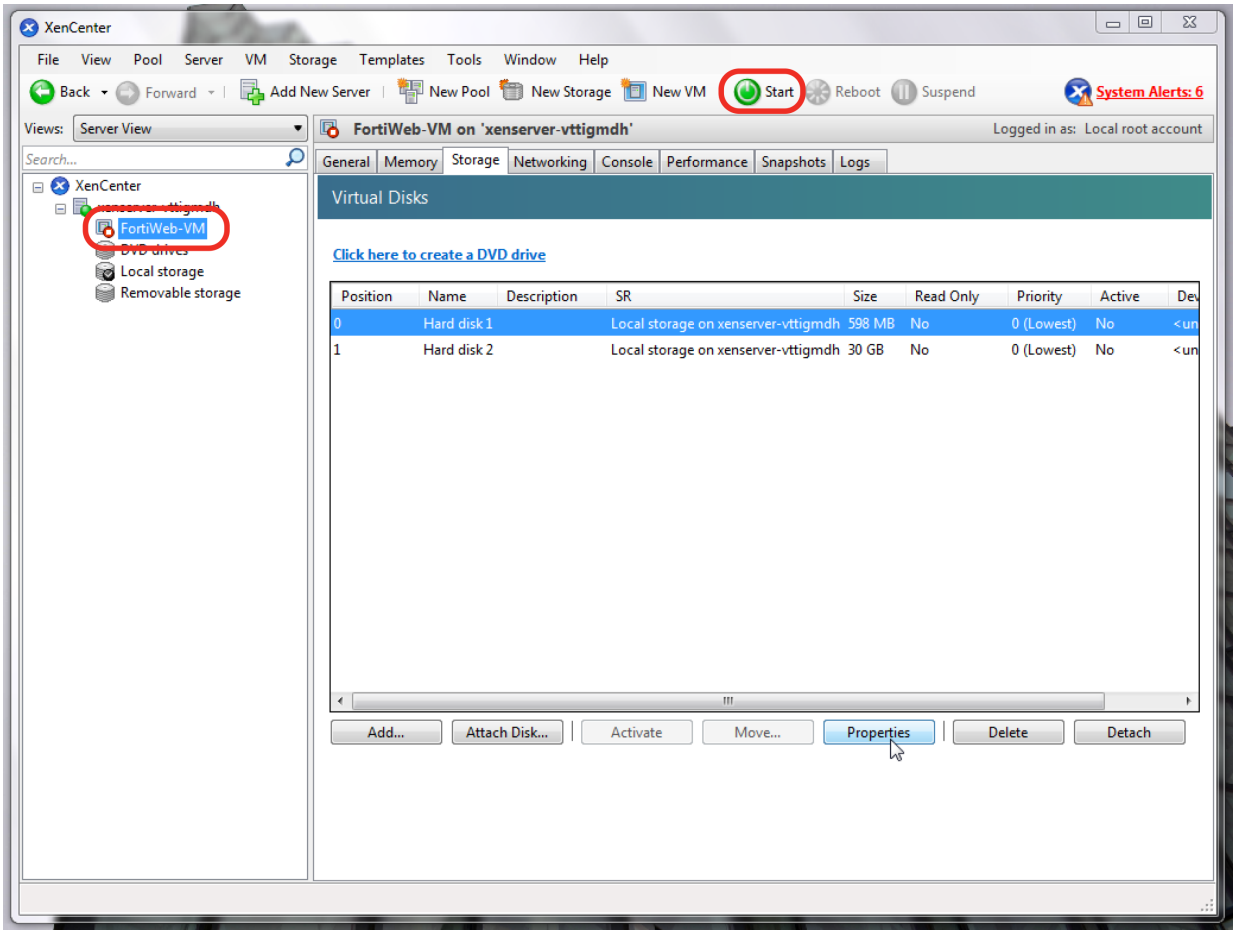
   In **User name**, type the name of your account on that server.

   In **Password**, type the password for your account on that server.

Click *Connect*.



4. In the pane on the left side, click the name of the virtual appliance, such as **FortiWeb-VM**.



5. Click **Start**.
6. Continue with Configuring access to FortiWeb's web UI & CLI on page 143.

Deploying FortiWeb-VM on Xen Project

FortiWeb-VM is deployed as a fully virtualized `domU` virtual machine.

To deploy FortiWeb-VM on a open source Xen Project hypervisor/XAPI cloud, you can use either the `dom0` virtual machine's:

- command line or
- desktop environment, such as GNOME or KDE

Once FortiWeb-VM is deployed, however, either your Xen server itself or your management computer **must** have a desktop environment. (`sudo xm console <domain_int>` using an alias to `/dev/pty` does not succeed. Instead, VNC is required to connect to FortiWeb-VM's virtual local console in Configuring access to FortiWeb's web UI & CLI on page 143.)

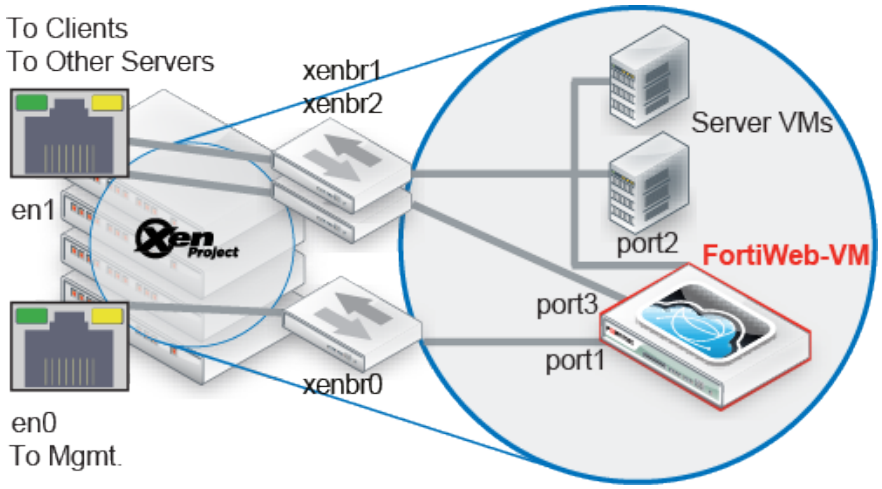
Bridging to one of the Xen server's physical network interfaces

If you have not yet installed the network bridge utilities required by Xen in order to bridge virtual machines' vNICs to the hypervisor's network connection, you must do that by installing the bridge network utilities and then editing the network interface configuration.

```
sudo apt-get install bridge-utils
sudo nano /etc/network/interfaces
```

When editing the network interface configuration, usually you should bind the bridge (in the `vif` example in Deploying via Virtual Machine Manager on page 92 or Deploying via dom0 command line on page 102, the bridge is `xenbr0`) to one of your network interfaces (e.g. `eth0`) in `/etc/network/interfaces`. Depending on the number of physical interfaces on the server and how you will map them to vNetworks, you may need to create multiple bridges.

The following table provides an example of how vNICs could be mapped to the physical network ports on a server with two physical NICs for a FortiWeb operating in reverse proxy mode.



Example: Network mapping for reverse proxy mode

Xen Project			FortiWeb-VM
Physical Network Adapter	**Network Mapping (vSwitch Port Group)**	**Virtual Network Adapter for FortiWeb-VM**	**Network Interface Name in Web UI/CLI**
eth0	xenbr0	Management	port1
eth1		External	port2
		Internal	port3
		External	port4

Below is a configuration example assuming the server has only one physical NIC, `eth0`:

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet manual

auto xenbr0
iface xenbr0 inet static
address 192.0.2.10
netmask 255.255.255.0
gateway 192.0.2.1
   #Enable line below for vSwitch with FortiWeb transparent mode
   #allow-hotplug xenbr0
```

Configuring the vNetwork for the transparent modes

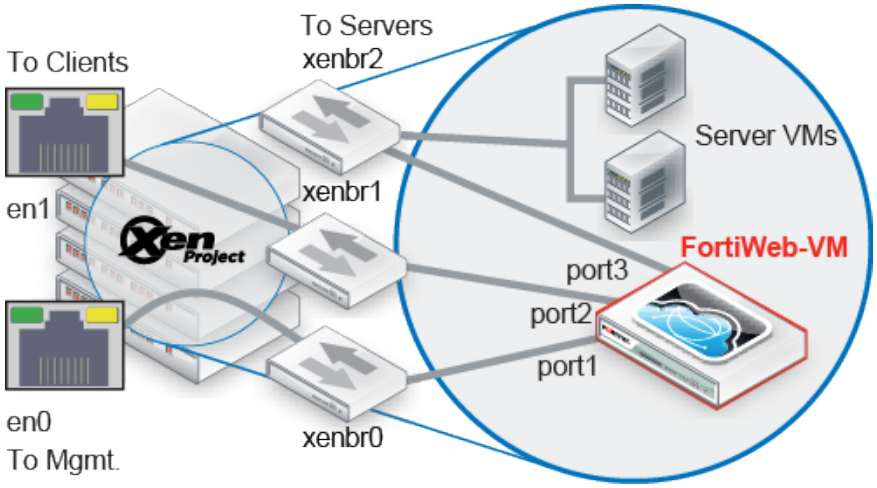
A simple Xen bridge configuration does **not** function with FortiWeb bridges (V-zones), which will be used if you deploy your FortiWeb-VM in either true transparent proxy or transparent inspection operation mode.

For information on how to choose the operation mode, see the setup instructions in the *FortiWeb Administration Guide*.

Use the following general configuration steps to support the transparent modes:

- To create the bridge, use one of the following to create two FortiWeb ports: one for the web server side and one for the client side:
  - 2 vSwitches or distributed vSwitches (dvSwitch)
  - 1 vSwitch that has 2 port groups with different VLAN IDs
- Set each vSwitch that you add to promiscuous mode and map each port group to a network adapter (vNIC) in the vNIC configuration (see Deploying via Virtual Machine Manager on page 92 or Deploying via dom0 command line on page 102)

Similar to a deployment that does not use virtual machines, connections between clients and servers are piped through two port groups (on two vSwitches or a single vSwitch) that comprise the bridge, with FortiWeb-VM in between them.



For instructions on how to create distributed vSwitches, see:

http://wiki.xen.org/wiki/Xen_Networking#Open_vSwitch

Creating the VM instance's logical volume

You must create the logical volume that FortiWeb-VM will use to store its vDisks. In this case, the logical volume is on the Xen server's local disk, but usually it is preferable to store it on an NFS or CIFS share.

To create a local logical volume

1. Connect to the command line in `dom0` on the Xen server where you will deploy FortiWeb-VM (for example, via an SSH client such as PuTTY).
2. Find the name of your `dom0` logical volume group. (Volume group is highlighted below in bold).

```
xenuser@LabXen:~$ sudo pvs
[sudo] password for xenuser:
PV VG Fmt Attr PSize PFree
/dev/sda5 LabXen-vg lvm2 a- 698.39g 673.45g
```

3. Create a logical volume. In this case, the logical volume is on the Xen server's local disk, but you could store it on an NFS or CIFS share.

```
sudo lvcreate -L 100G -n fortiweb-vm /dev/LabXen-vg
```

where you would replace:

- `100G` — The amount of disk space to allocate to FortiWeb-VM's vDisk in gigabytes.
- `fortiweb-vm` — The name of your virtual machine, as it appears in Virtual Machine Manager or when you use the `xm` command to create the virtual machine.
- `LabXen-vg` — The name of your `dom0` volume group according to the output of the `sudo pvs` command.

Deploying via Virtual Machine Manager

If you have not yet installed a graphical centralized management tool for Xen on your management computer, begin by installing it. Multiple clients exist for managing Xen Project servers. In these instructions, we use Virtual Machine Manager.

On Debian-related Linux distributions, to install Virtual Machine Manager, open a terminal and enter:

```
sudo apt-get install virt-manager
```

On Red Hat-related Linux distributions, the command is :

```
sudo yum virt-manager
```

This centralized manager includes a Xen client for connecting to a remote Xen Project hypervisor to deploy FortiWeb-VM. It also includes a built-in VNC client that you will need later in order to connect to FortiWeb-VM's local console and configure its network connection. When the download and installation is complete, if you are not already logged into your desktop environment (GNOME, KDE, xfce, etc.), start X Windows and log in.

To enable Virtual Machine Manager to connect to your Xen server, you must also modify the **server's** configuration file (usually `/etc/xen/xend-config.sxp`). Un-comment these lines (remove the hash (`#`) from the beginning) and change '`no`' to '`yes`':

```
(xend-unix-server yes)
(xend-unix-path /var/lib/xend/xend-socket)
```

To deploy the VM image using Virtual Machine Manager

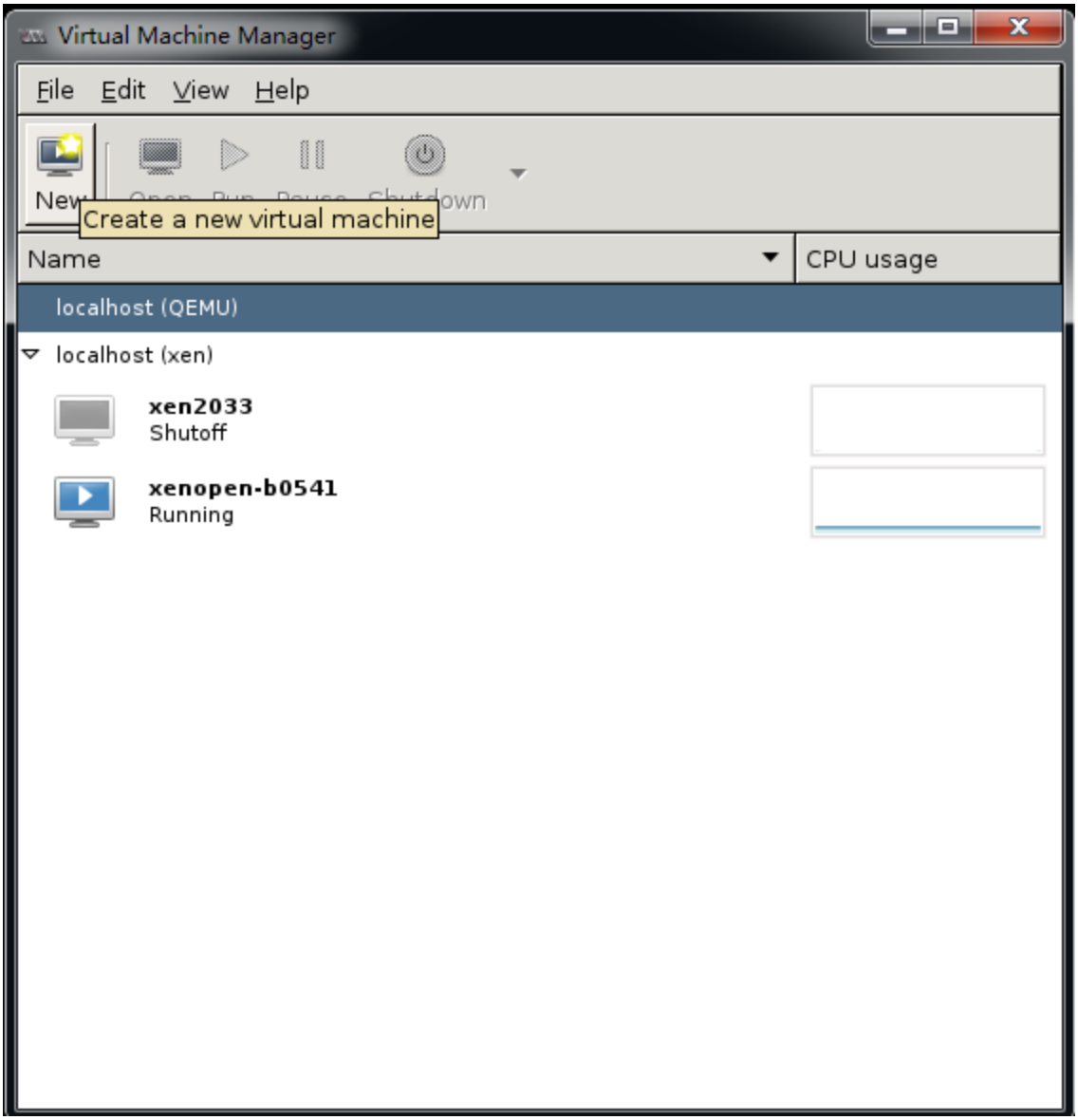
1. On your management computer, open a terminal application and enter the command to extract the package to a folder, then start Virtual Machine Manager:

   ```
   unzip FWB_XENOPEN-v500-build-0057-FORTINET.out.xenopensource.zip
   sudo virtu-manager
   ```

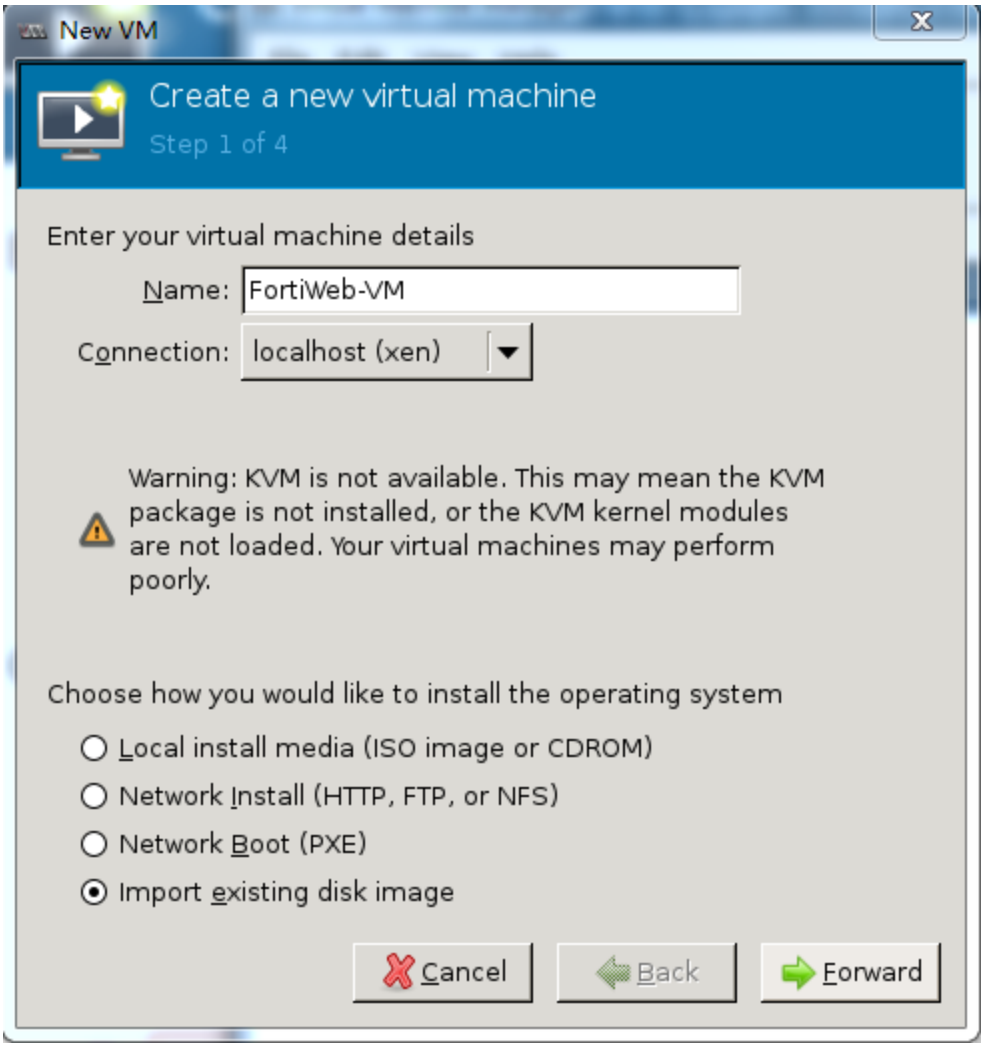
   The application will open in your desktop environment, so its appearance may vary slightly.

2. Go to **File > Add Connection** and connect to the Xen server where you will deploy the VM.

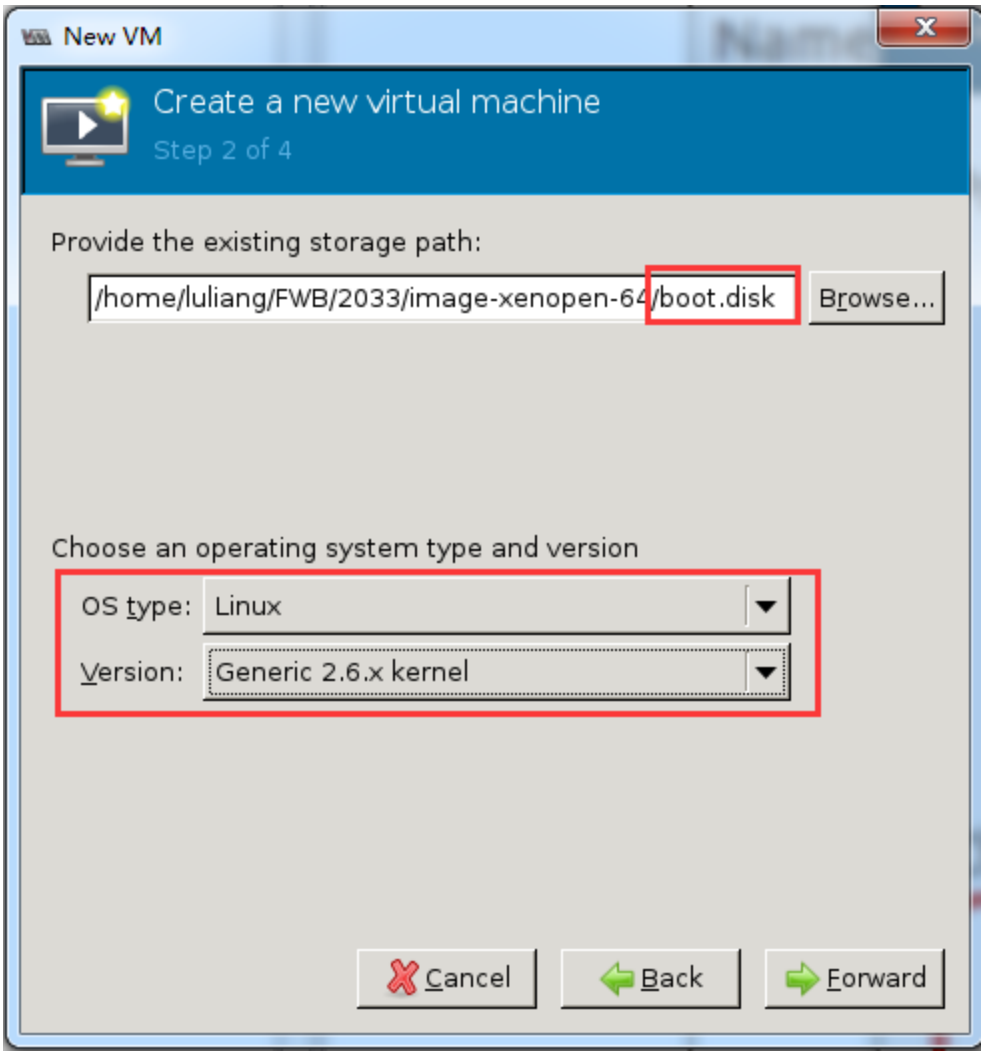
3. Click the **Name** icon to open the wizard for a new virtual machine.



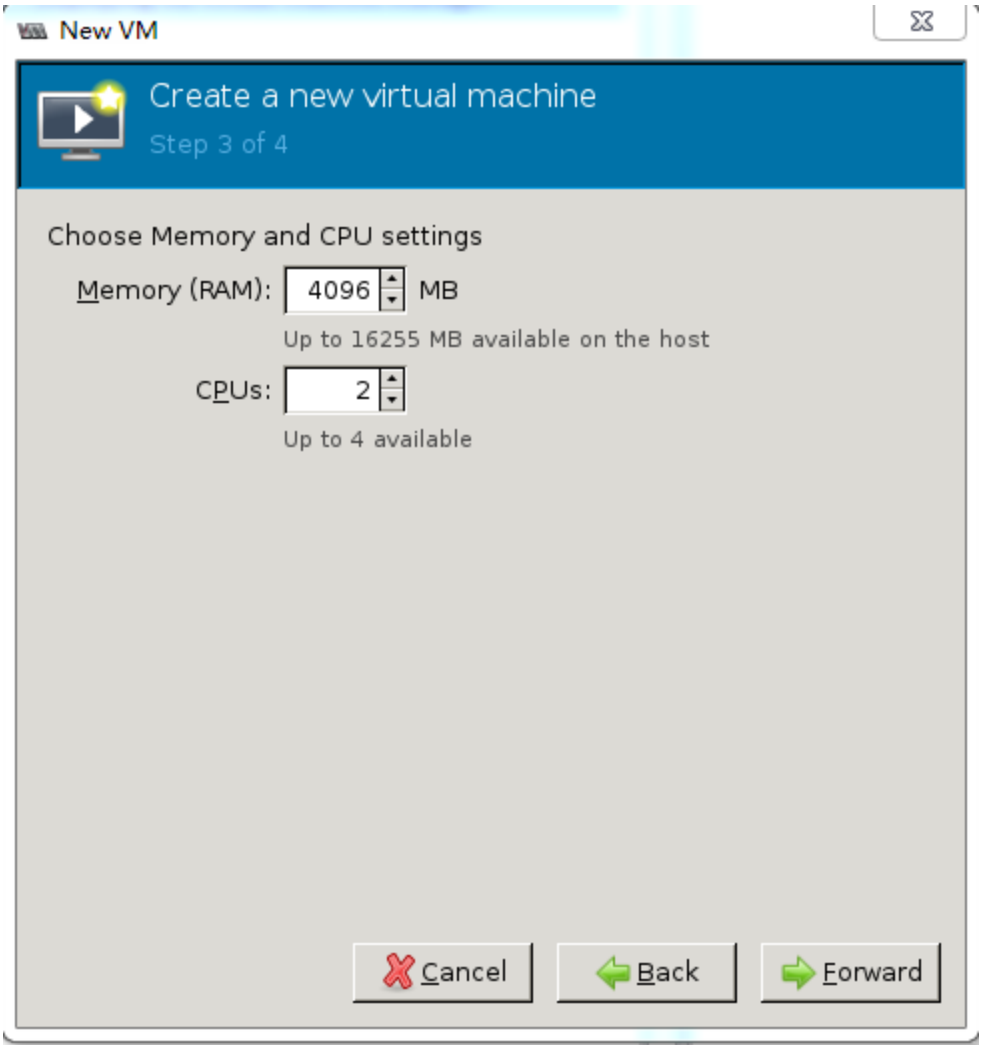
4. In **Name**, type a unique descriptive name for this instance of FortiWeb-VM as it will appear in Virtual Machine Manager's inventory, such as `FortiWeb-VM`. If you will deploy multiple instances of this file, consider a naming scheme that will make each VM's purpose or IP address easy to remember. (This name will not be used as the host name, nor will it appear within the FortiWeb-VM web UI.) Select **Import existing disk image**, then click **Forward**.



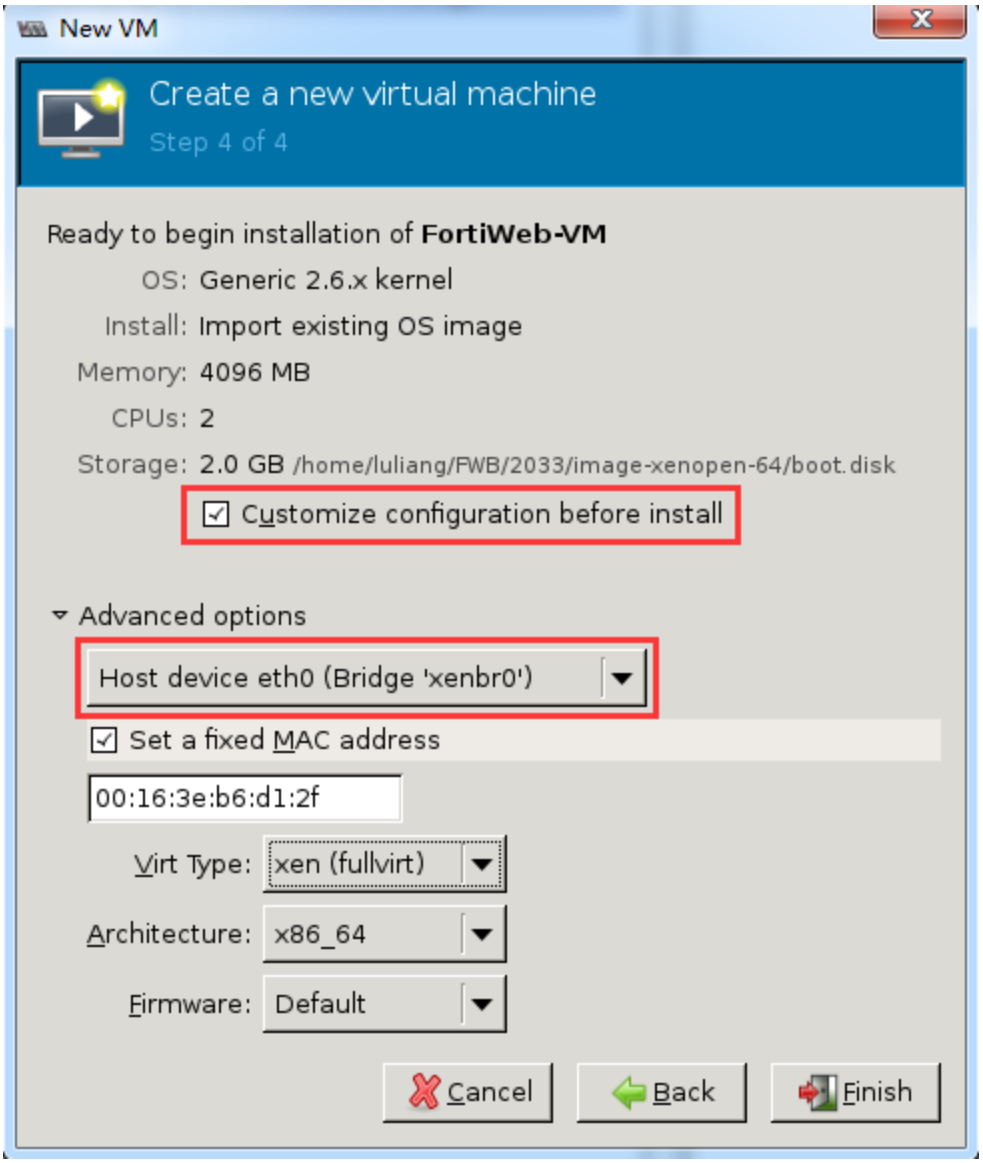
5. Click Browse and locate the `bootdisk.img` file. In **OS type**, select **Linux**, then in **Version**, expand the list to show all distributions, then select **Generic 2.6.x kernel**, and click **Forward**.



6. Adjust the vRAM and vCPU settings to be appropriate for your deployment. Fortinet recommends a minimum of 2048 MB vRAM and 1 vCPU. Valid vCPU values range from 1 to 8, depending on your FortiWeb-VM license. Click **Forward**.



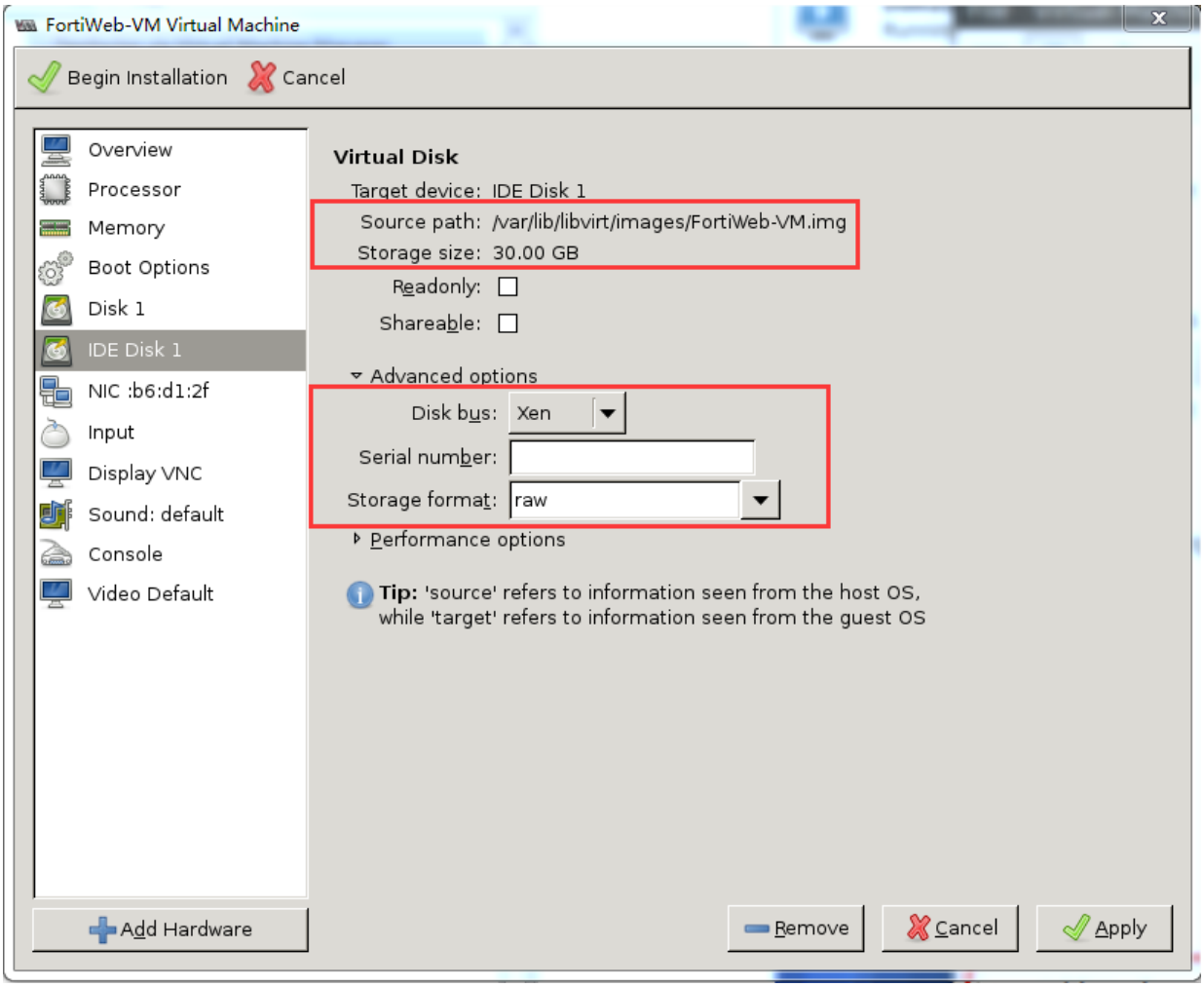
7. Mark the **Customize configuration before install** check box. Also click to expand **Advanced options**, then click the drop-down menu to change NAT to **Specify shared device name** and in **Bridge name**, enter the name of the Xen bridge (e.g. `xenbr0`). For more information on network mappings, see Mapping the virtual NICs (vNICs) to physical NICs. **Virt Type** should be **xen (fullvirt)**. Click **Finish**.



A new dialog will appear where you can add the other vDisk and vNICs.

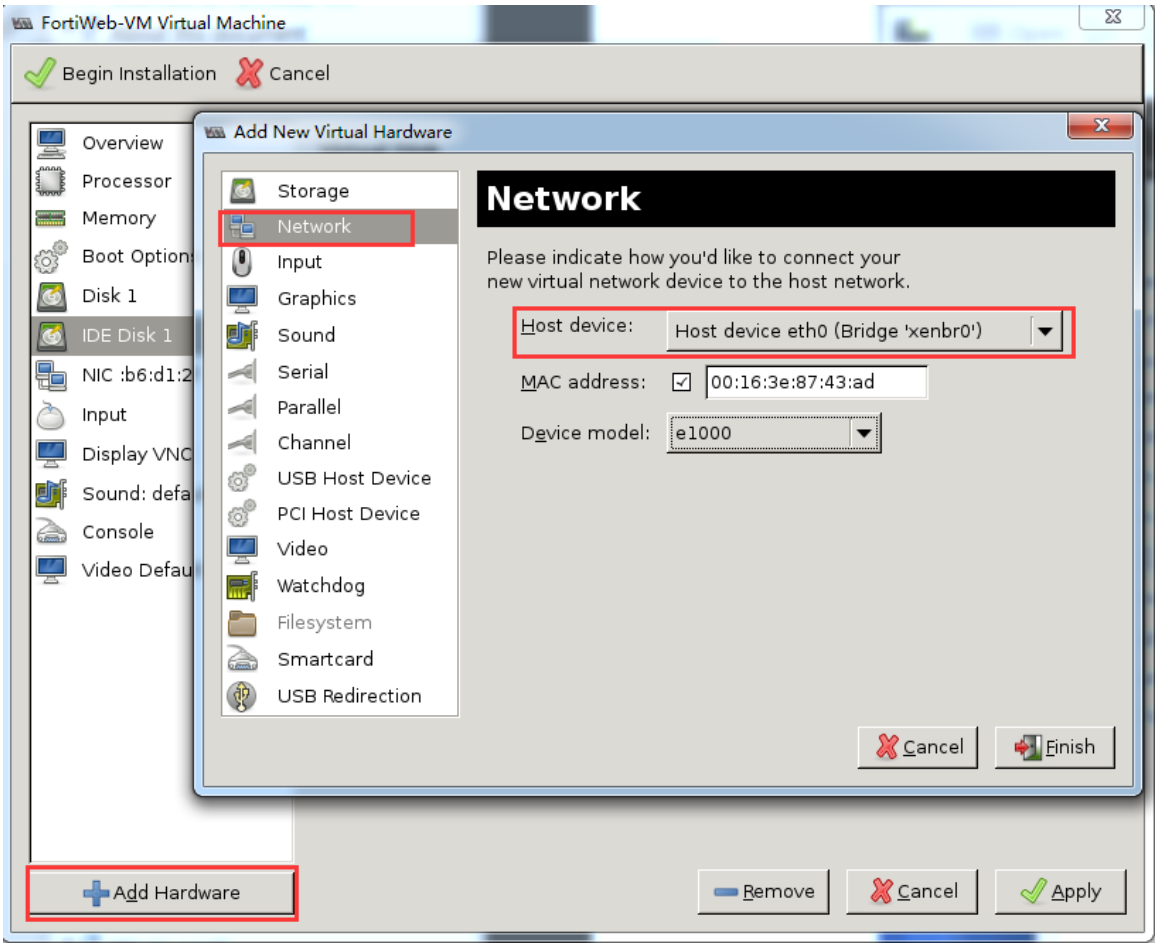
8. In the menu on the left, select the virtual disk. In **Advanced options**, configure `boot.disk` to be a virtual disk (raw). Then click the **Add Hardware** button and select **Create a disk image on the computer's hard drive**. For **Storage format**, select **raw**.


FortiWeb-VM Virtual Machine
Begin Installation
Cancel
Overview
Processor
Memory
Boot Options
Disk 1
NIC :b6:d1:2f
Input
Display VNC
Sound: default
Console
Video Default
Add Hardware
Add New Virtual Hardware
Storage
Network
Input
Graphics
Sound
Serial
Parallel
Channel
USB Host Device
PCI Host Device
Video
Watchdog
Filesystem
Smartcard
USB Redirection
Storage
Please indicate how you would like to assign space on the host system for your virtual storage device.
Create a disk image on the computer's hard drive
30.0 GB
1776.5 Gb available in the default location
Allocate entire disk now
Select managed or other existing storage
Browse...
Device type: IDE disk
Cache mode: default
Storage format:
Cancel
Finish
Security
Cancel
Apply

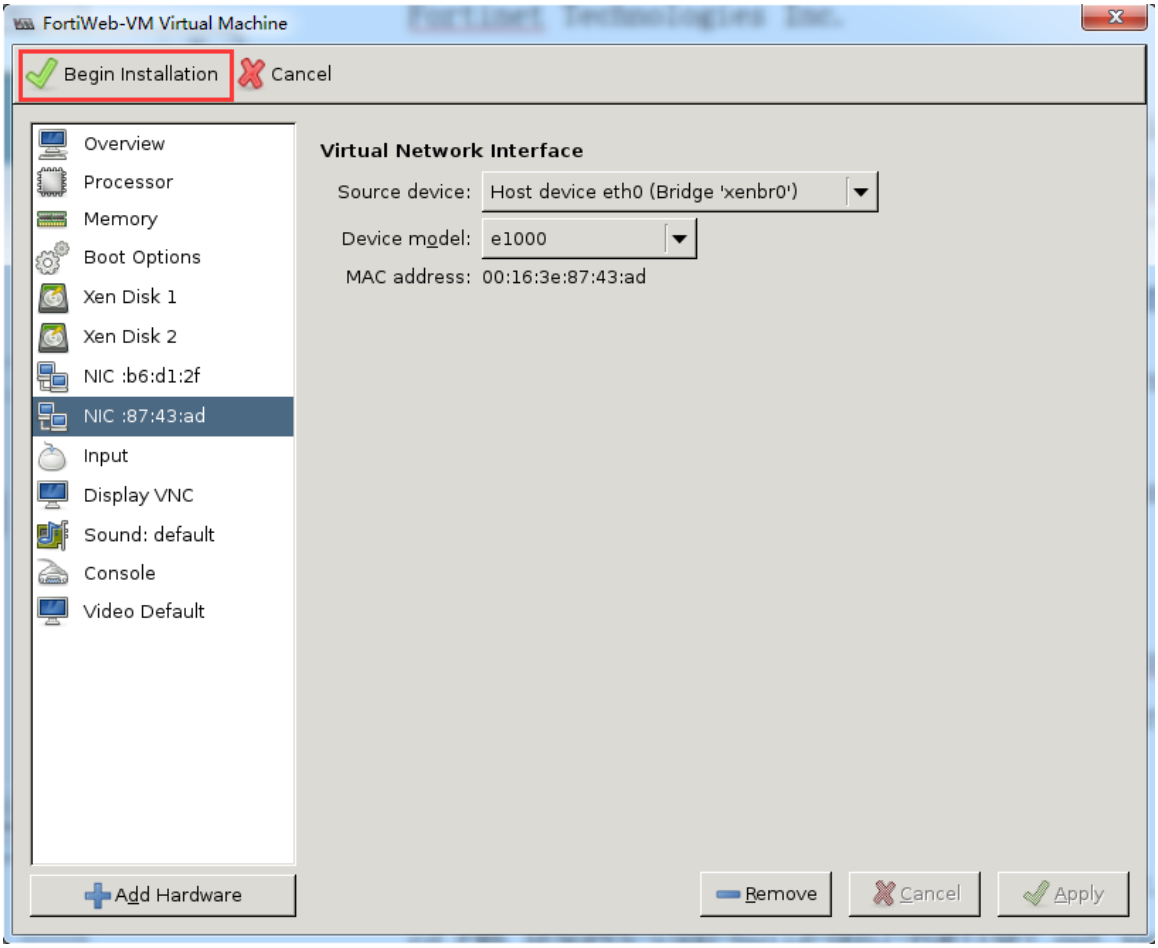


9. In the menu on the left, click **Add Hardware** and add another virtual network adapter that is bound to the bridge. (If the server has more than one physical network adapter, depending on your network topology, you may want to bind these vNICs to different bridges. If you will be deploying FortiWeb-VM in transparent mode and have a vSwitch controller, you must also configure that. See Mapping the virtual NICs (vNICs) to physical NICs on page 76 and Configuring the vNetwork for the transparent modes on page 81.)

Repeat this step again until you have 4 vNICs, then click **Apply**.



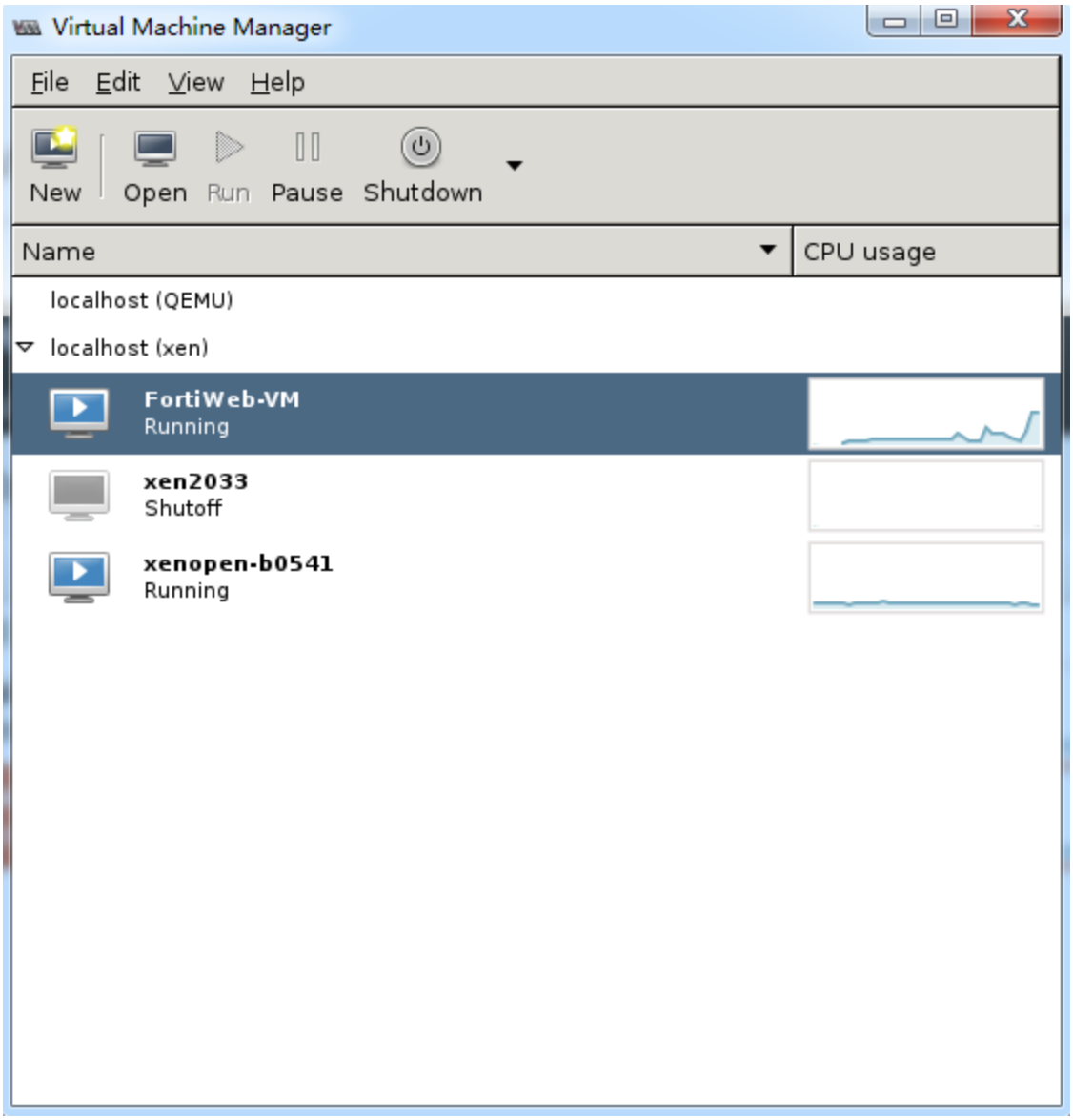
10. Click **Begin Installation** to send the FortiWeb-VM image and its VM settings to the Xen server.



The client connects to the VM environment, and deploys the image to it. Time required depends on your computer's hardware speed and resource load, and also on the file size and speed of the network connection, but might take 15 minutes to complete.

When complete, the deployment should appear in the list of deployed VMs for that Xen server, in the pane on the left side of Virtual Machine Manager.

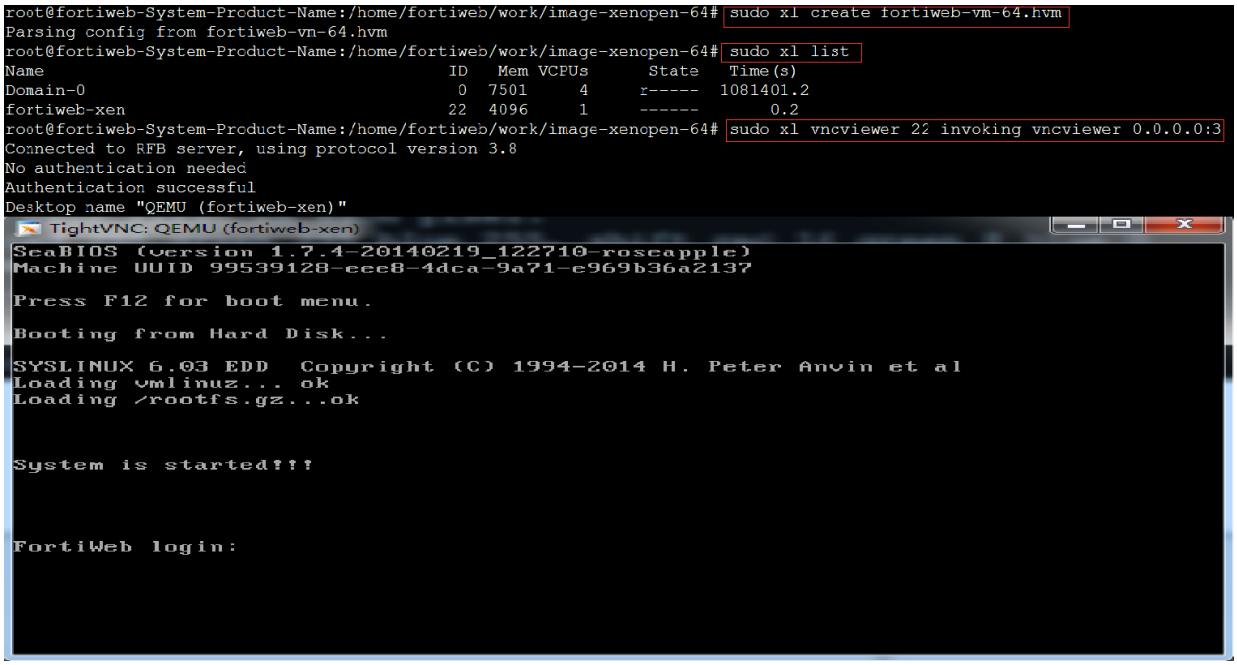
11. To power on the VM, click the **Play** button.



12. Continue with Configuring access to FortiWeb's web UI & CLI on page 143.

Deploying via dom0 command line

Connect to the command line of your `dom0` guest. For example, you may be able to use PuTTY to make an SSH connection to the Xen server's IP address, or you may use a local GNOME Terminal application.



Next, unpack the file that you downloaded from Fortinet, and open the configuration file in a plain text editor such as `nano`.

```
unzip FWB_XENOPEN-v500-build-0057-FORTINET.out.xenopensource.zip
cd FWB_XENOPEN-v500-build-0057-FORTINET.out.xenopensource/
nano fortiweb.hvm
```

Then edit these lines in `fortiweb-vm-64.hvm`:

```
memory = 4096
vcpus = 2
vif = [ 'type=netfront, bridge=xenbr0', 'type=netfront, bridge=xenbr0', 'type=netfront,
    bridge=xenbr0', 'type=netfront, bridge=xenbr0', ]
disk = ["format=raw, vdev=xvda, access=rw, target=boot.disk", 'format=qcow2, vdev=xvdb,
    access=rw, target=log.qcow2']
```

If FortiWeb-VM will be running in transparent mode, the vNIC (`vif`) must be configured differently to include vSwitches and vNICs in promiscuous mode. For instructions, see:

http://wiki.xen.org/wiki/Xen_Networking#Open_vSwitch

For more information on network mappings, see Example: Network mapping for reverse proxy mode on page 90.

Alternatively to locally stored disk images, you can reference an NFS or CIFS share:

```
#Mount point on the server's local file system
root = "/dev/nfs"
nfs_server = '192.0.2.100'
#Root directory on the NFS server
nfs_root = '/path/to/directory'
```

Configure virtual hardware settings to allocate appropriate resources for the size of your deployment before powering on the virtual appliance. For details, see the documentation for the open source Xen Hypervisor.

Change the value if necessary to allocate enough vCPUs for the size of your deployment. Valid vCPU values range from 1 to 8, depending on your FortiWeb-VM license.

Similarly, FortiWeb-VM for Xen Project comes pre-configured to use 4 GB of vRAM (`memory`). However, this is not enough for most deployments. Change this value to be appropriate for your deployment. The valid range is from 4 GB to 16 GB.

If you configure the virtual appliance's storage to be internal (that is, local, on its own vDisk), resize the vDisk before powering on. The FortiWeb-VM package that you downloaded includes pre-sized VMDK (Virtual Machine Disk Format) files. However, they are only 32 GB, which is not large enough for most deployments. Resize the vDisk before powering on the virtual machine.

This step is not applicable if the virtual appliance will use external network file system (such as NFS or CIFS) datastores.

Depending on your Xen `dom0` platform, you may also need to reconfigure `fortiweb-vm-64.hvm` with the path to your `hvmloader`. For example, this may be correct for CentOS or Red Hat Linux:

```
kernel = "/usr/lib/xen/boot/hvmloader
```

but this is required by Ubuntu 12.0.4 LTS:

```
kernel = "/usr/lib/xen-4.1/boot/hvmloader
```

Apply the changes by rebooting or restarting networking. (In some cases rebooting is required: `sudo /etc/init.d/networking restart` may not delete your old IP address from `eth0` and therefore not correctly bring up all interfaces.)

Run these commands to deploy the VM, power it on, and show its Xen domain ID number (highlighted below in bold):

```
xenuser@LabXen:/$ sudo xm create fortiweb.hvm
xenuser@LabXen:/$ sudo xm list
Name ID Mem VCPUs State Time(s)
Domain-0 0 5877 4 r----- 1556.9
fortiweb-vm 2 2048 2 -b---- 126.8
```

If your `dom0` is Ubuntu 12.04 and/or when creating the VM, you receive this error:

```
Error: Domain 'fortiweb-xen' does not exist.
```

and if `/var/log/xen/qemu-dm-fortiweb-xen.log` contains this line:

```
Could not read keymap file: '/usr/share/qemu/keymaps/en-us'
```

then the key mapping is not in its expected location. Enter this line:

```
sudo ln -s /usr/share/qemu-linaro /usr/share/qemu
```

then retry the command to create FortiWeb-VM.

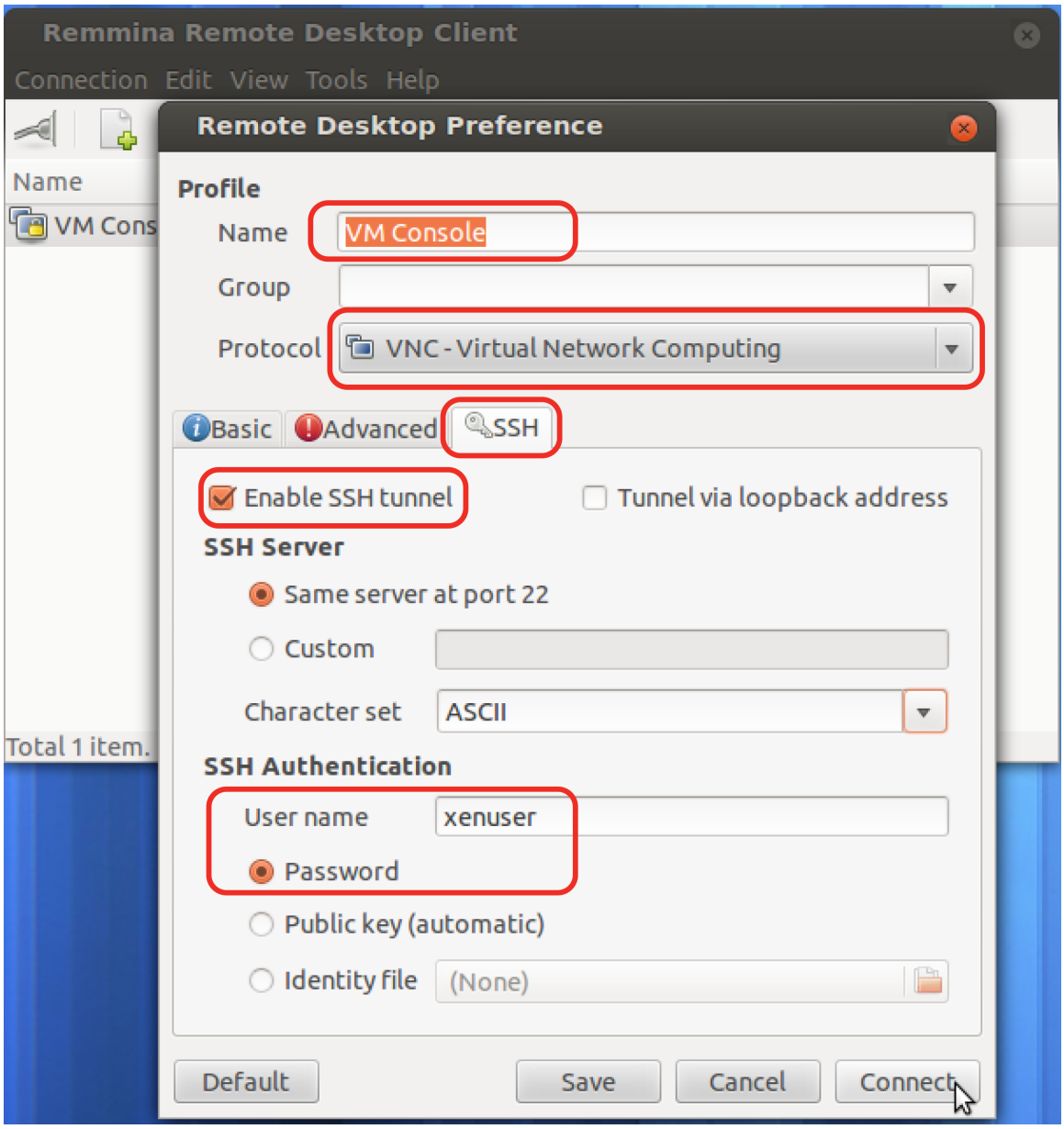
Since VNC listening port numbers are dynamically allocated to guest VMs, use the domain ID number in the output from the previous command to run this command to show the current VNC listening port number and IP address for FortiWeb-VM:

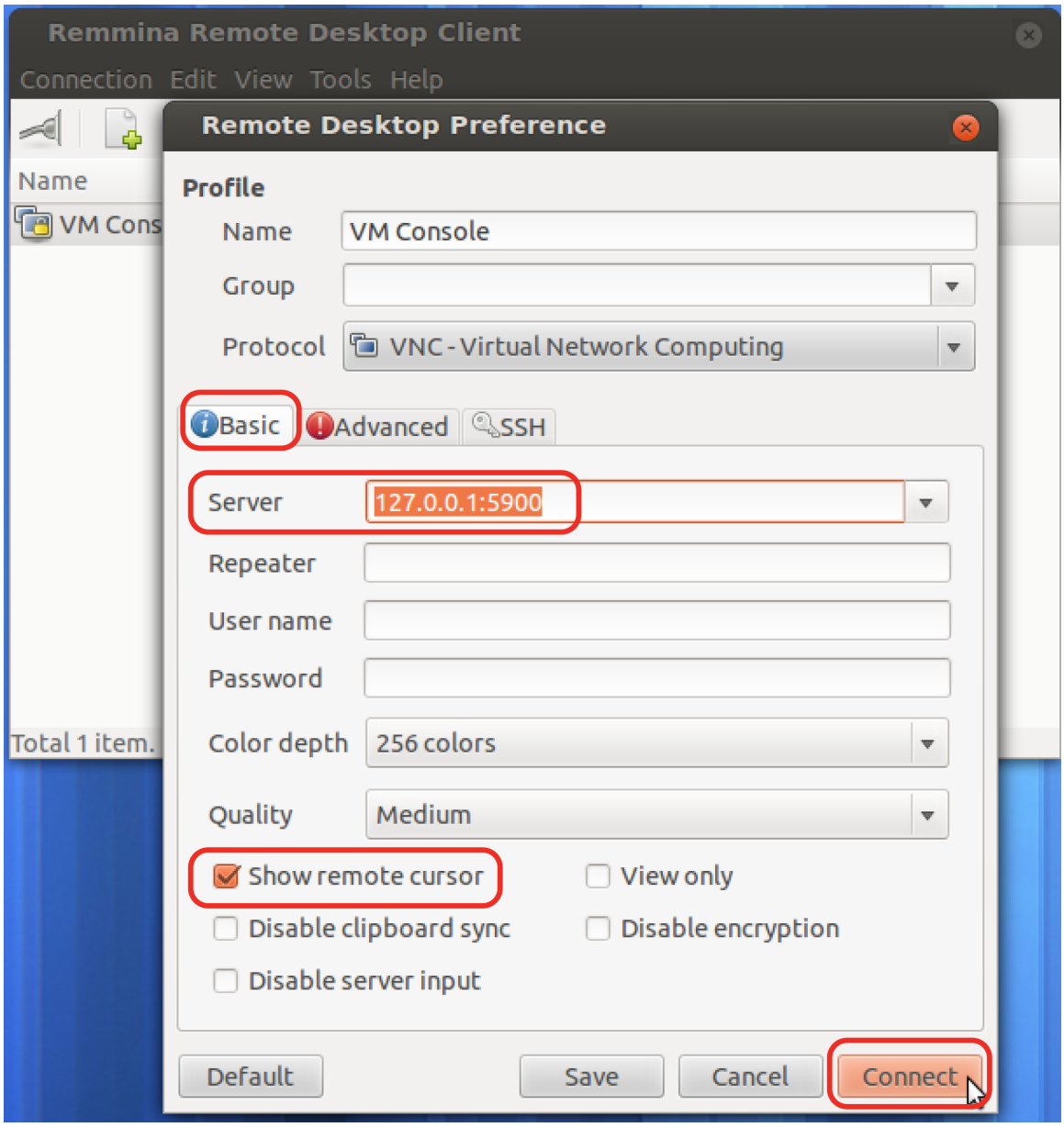
```
xenuser@LabXen:/$ sudo xenstore-ls /local/domain/2/console
port = "4"
limit = "1048576"
type = "ioemu"
vnc-port = "5900"
vnc-listen = "127.0.0.1"
tty = "/dev/pts/5"
```

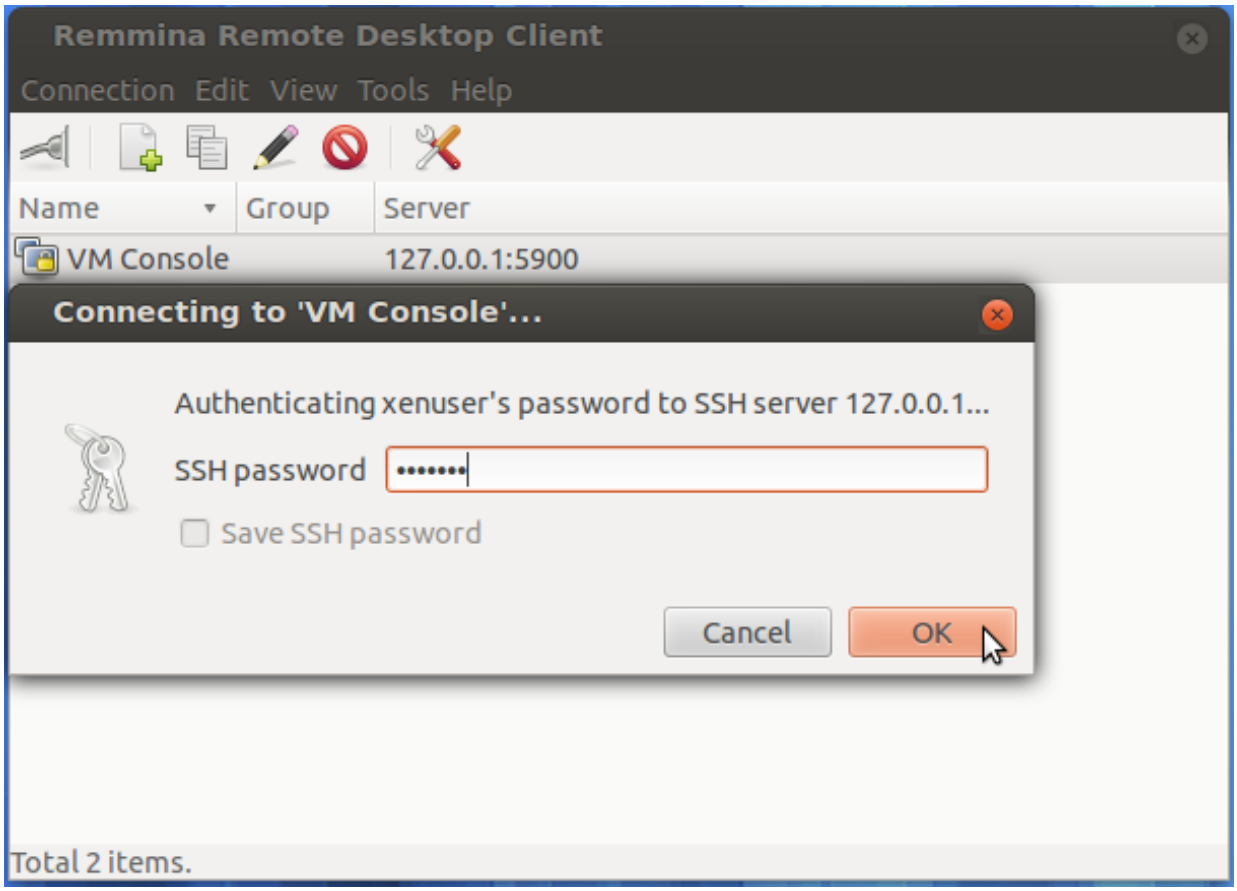
Finally, on your management computer, install and start a VNC viewer and connect to the Xen server's IP address and listening port number for VNC. (In the images below, the VNC viewer is installed in `dom0` on the Xen server that is hosting FortiWeb-VM, so the VNC viewer connects to 127.0.0.1. If connecting from your management computer, replace this with the IP address of your Xen server.) For example, on a Debian or Ubuntu Linux management computer, you could use these commands:

```
sudo apt-get install remmina
remmina
```

You **must** run this command from a terminal with an X Windows environment such as GNOME Terminal in order for it to be able to open the VNC viewer window.


Remmina Remote Desktop Client
Connection Edit View Tools Help
Name
VM Cons
Total 1 item.
Remote Desktop Preference
Profile
Name
VM Console
Group
Protocol
VNC - Virtual Network Computing
Basic
Advanced
SSH
Enable SSH tunnel
Tunnel via loopback address
SSH Server
Same server at port 22
Custom
Character set
ASCII
SSH Authentication
User name
xenuser
Password
Public key (automatic)
Identity file
(None)
Default
Save
Cancel
Connect


Remmina Remote Desktop Client
Connection Edit View Tools Help
Name
VM Cons
Total 1 item.
Remote Desktop Preference
Profile
Name
VM Console
Group
Protocol
VNC - Virtual Network Computing
Basic
Advanced
SSH
Server
127.0.0.1:5900
Repeater
User name
Password
Color depth
256 colors
Quality
Medium
Show remote cursor
View only
Disable clipboard sync
Disable encryption
Disable server input
Default
Save
Cancel
Connect



Continue with Configuring access to FortiWeb's web UI & CLI on page 143.

Deploying FortiWeb-VM on Hyper-V

You deploy FortiWeb-VM on Hyper-V by importing a virtual machine.

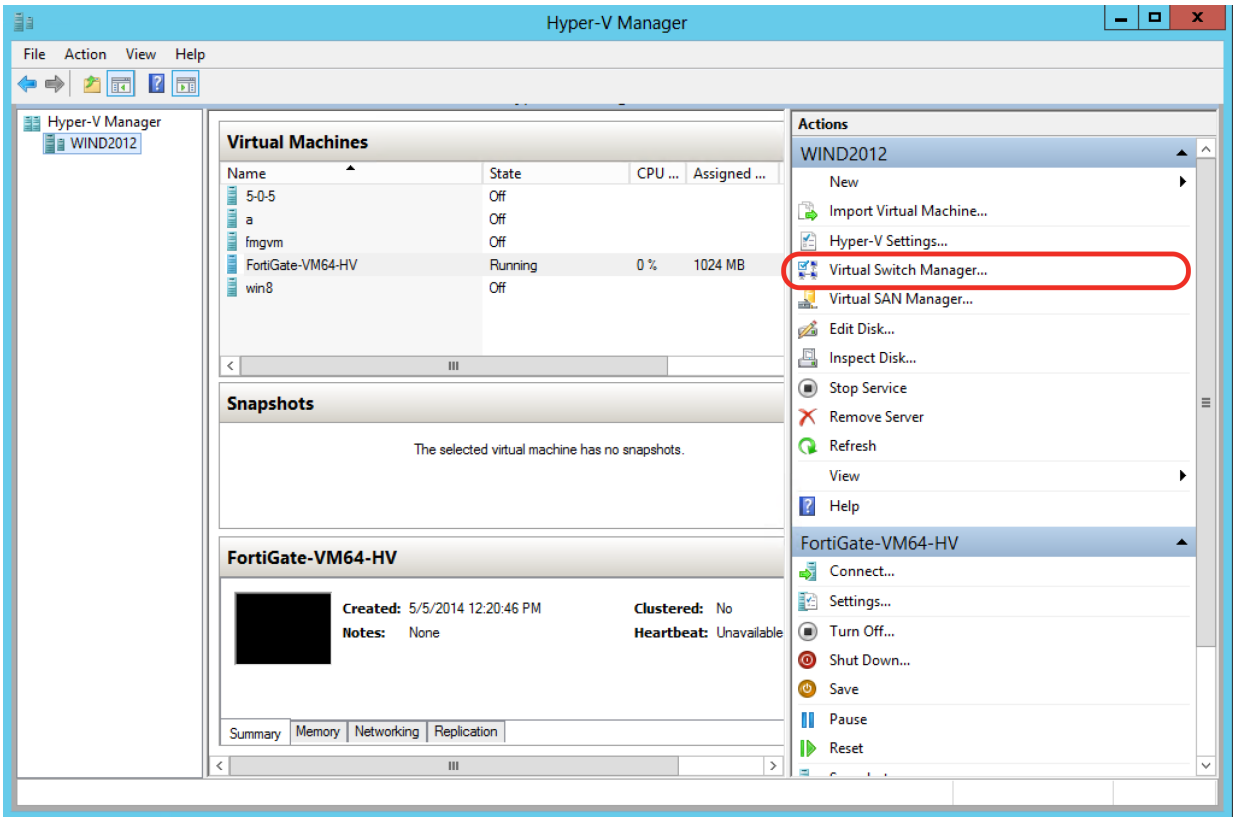
These instructions create a virtual switch named `vmnet`. The FortiWeb-VM virtual machine you import uses a virtual switch with this name by default.

Alternatively, you can use an existing virtual switch or one with different name. You are prompted to select the switch you want to use when you import the virtual machine.

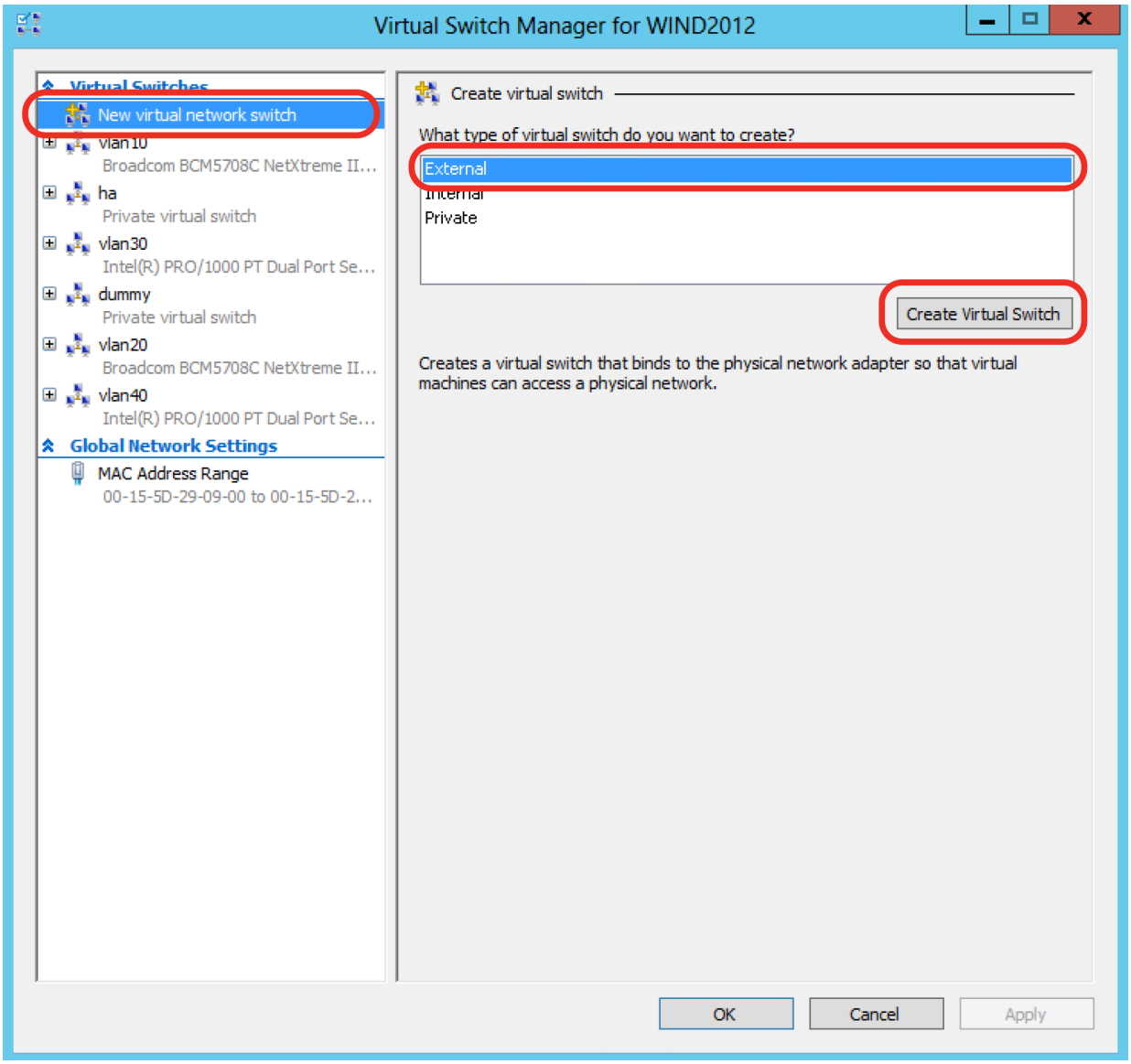
Import the FortiWeb-VM virtual machine

To import the FortiWeb-VM virtual machine

1. In the Hyper-V Manager, under **Actions**, click **Virtual Switch Manager**.



2. Under **Virtual Switches**, click **New virtual network switch**, click **External**, and then click **Create Virtual Switch**.



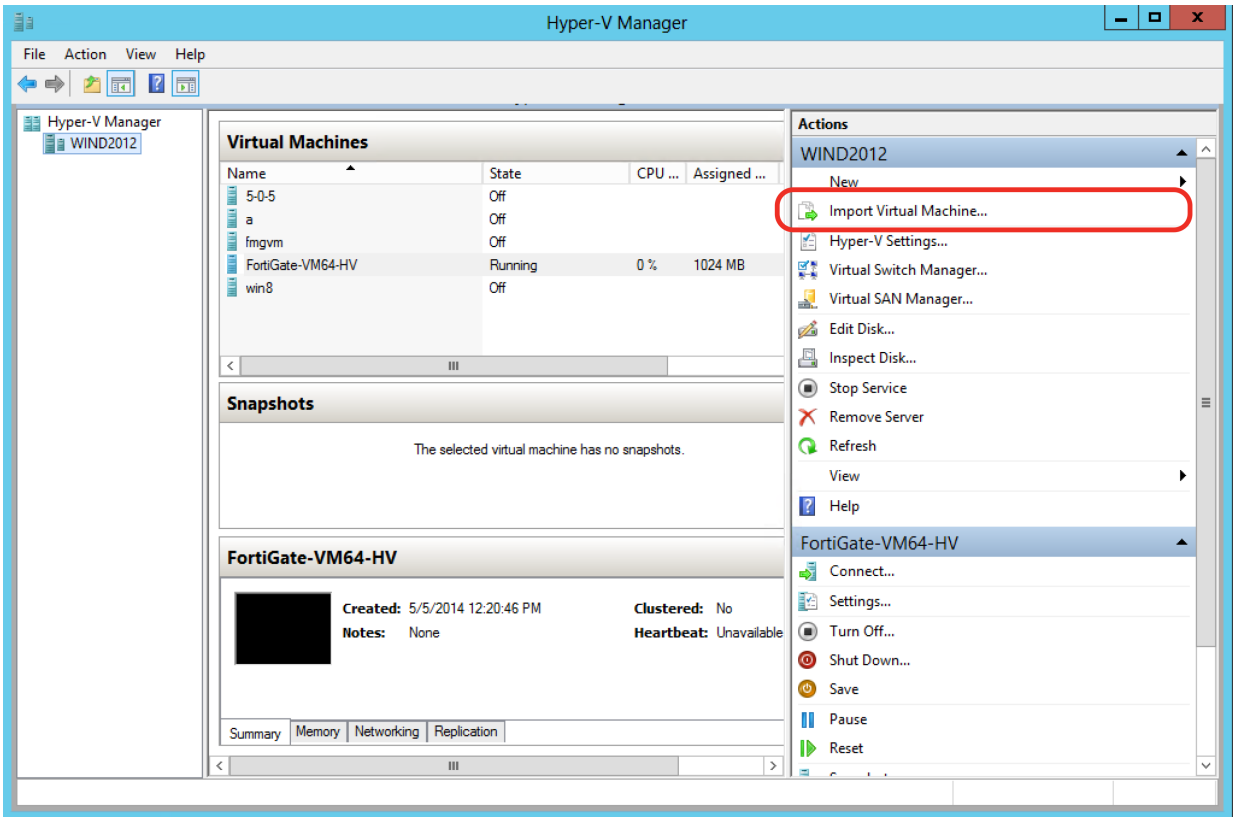
3. Under **Virtual Switch Properties**, for **Name**, enter `vmnet`.

   For all other settings, use the default values.

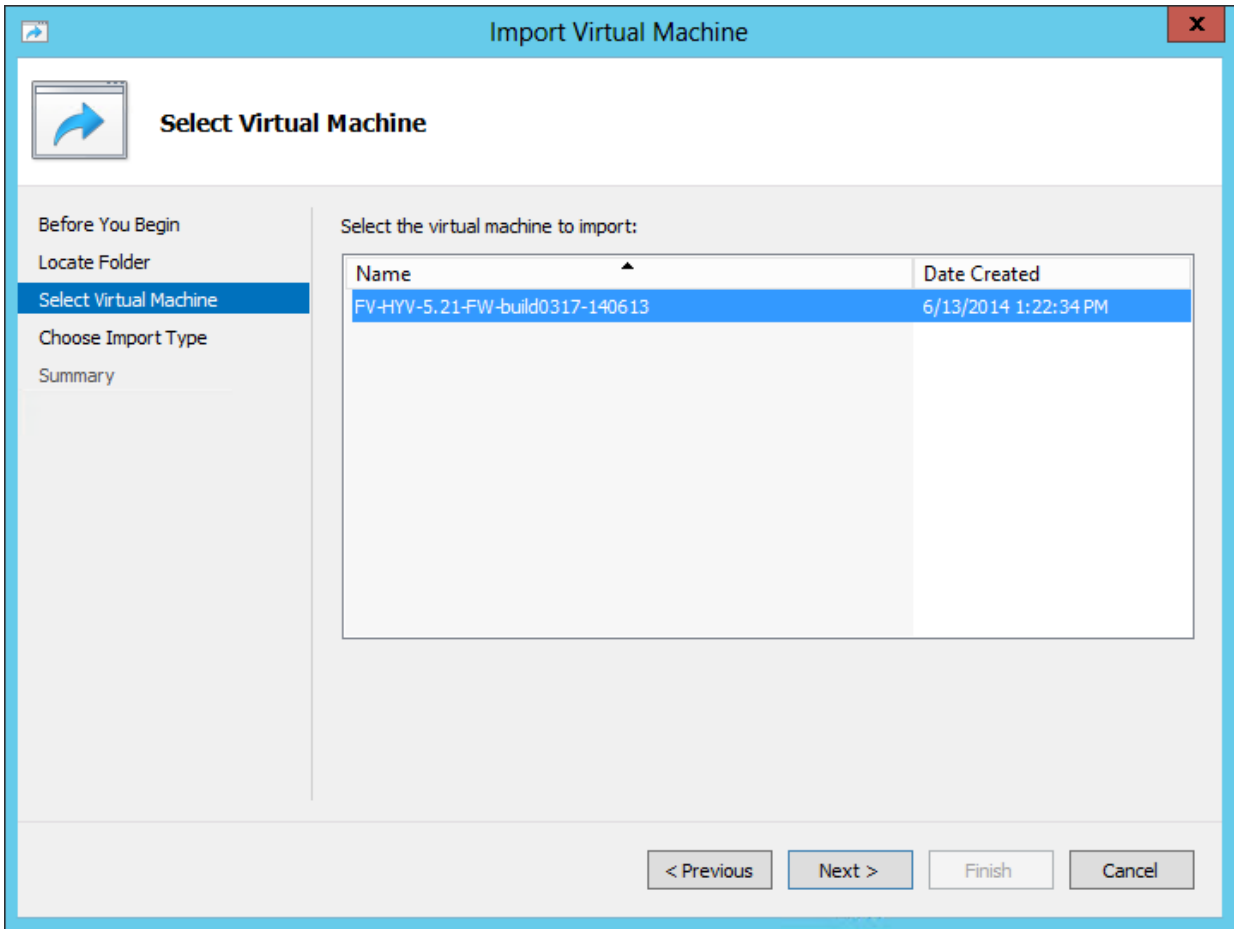
4. Click **OK**.

5. Extract the `.zip` archive's contents to a folder that you can access from the Hyper-V Manager.

6. In Hyper-V Manager, under **Actions**, click **Import Virtual Machine**.



7. In the **Import Virtual Machine** wizard, navigate to the **Locate Folder** page.
8. For **Folder**, specify the folder that contains the contents of the `.zip` file, and then click **Next**.
9. On the **Select Virtual Machine** page, select the name of the FortiWeb-VM virtual machine, and then click **Next**.



10. On the **Choose Import Type** page, select **Copy the virtual machine (create a new unique ID)**, and then click **Next**.
11. On the **Choose Folders for Virtual Machine Files** page, preserve the default values or specify the folders where you want to store the virtual machine. Then, click **Next**.
12. On the **Locate Virtual Hard Disks** page, for **Location**, specify the folder where you extracted the contents of the `.zip` file, and then click **Next**.
13. On the **Choose Storage Folders to Store Virtual Hard Disks** page, preserve the default value or specify a different folder**.** Then, click **Next**.
14. On the **Completing Import Wizard** page, review the settings, and then click **Finish**.

Resizing the virtual disk

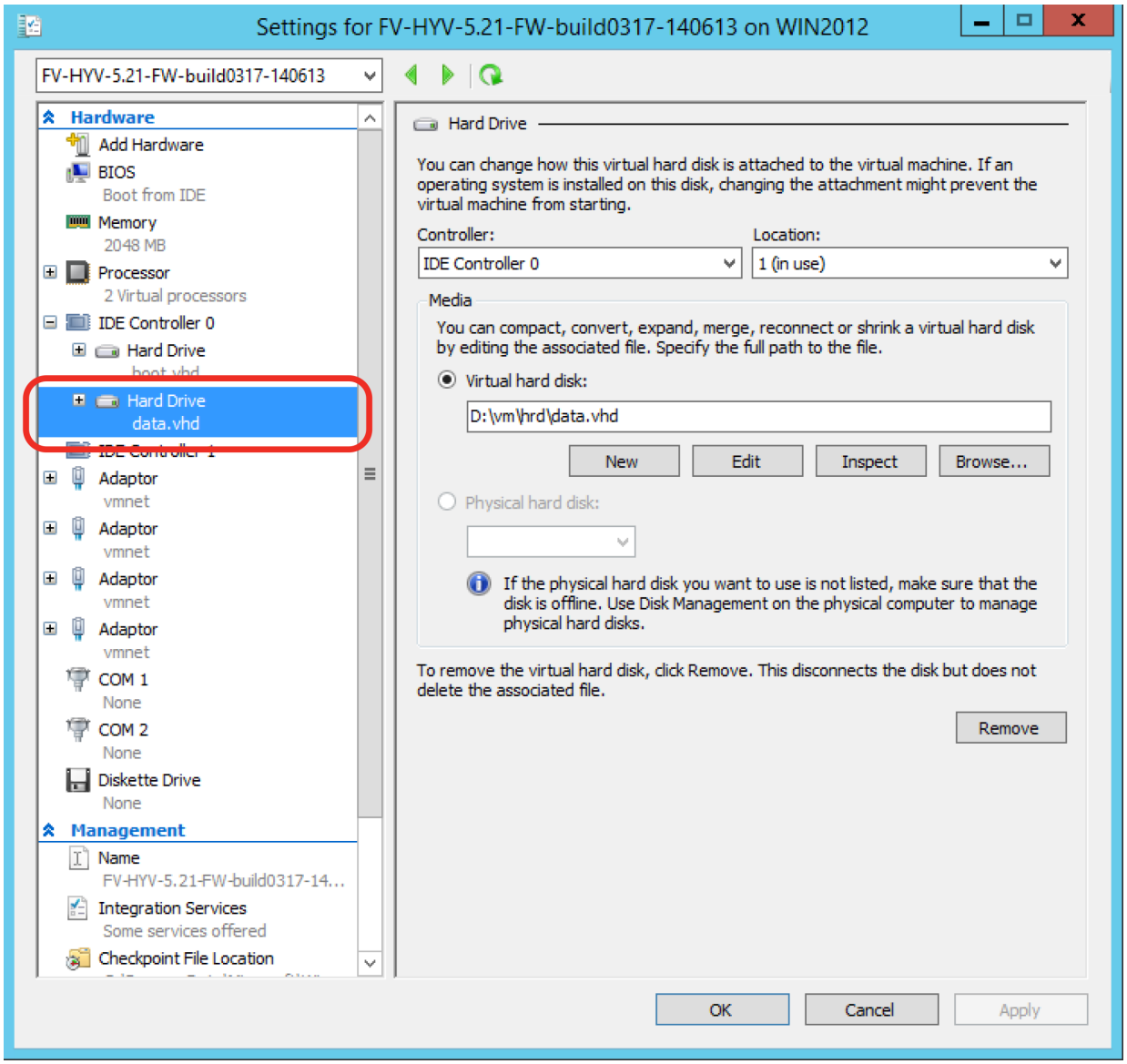
The virtual disk size of the imported FortiWeb-VM virtual machine is 30G (the default size for a Hyper-V virtual machine).

If you are resizing the disk for an existing deployment of FortiWeb-VM, back up the logs and other non-configuration data before beginning this procedure. **Formatting the disk deletes all data on that disk.** For backup instructions, see the *FortiWeb Administration Guide*.

You shut down the FortiWeb-VM to resize the vDisk.

To increase the size of the virtual hard disk

1. Shut down the FortiWeb-VM virtual machine (**Actions > Shut Down**).
2. Select the FortiWeb-VM virtual machine in the list of machines, and then, under **Actions**, click **Settings**.
3. Under **Hardware**, expand the IDE Controller item that contains the machine's hard drives, and then select the hard drive `data.vhd`.



4. In the hard drive settings, under Media, ensure that **Virtual hard disk** is selected, click **Edit**, and then use the Edit Virtual Hard Disk wizard to expand the size of the virtual disk.
5. Start the virtual machine (**Actions > Start**).
6. Using the CLI, log in to FortiWeb and use the following command to reformat the log disk:

   ```
   execute formatlogdisk
   ```

   After a reboot, the disk operates at the new size.

Configuring the number of virtual CPUs (vCPUs)

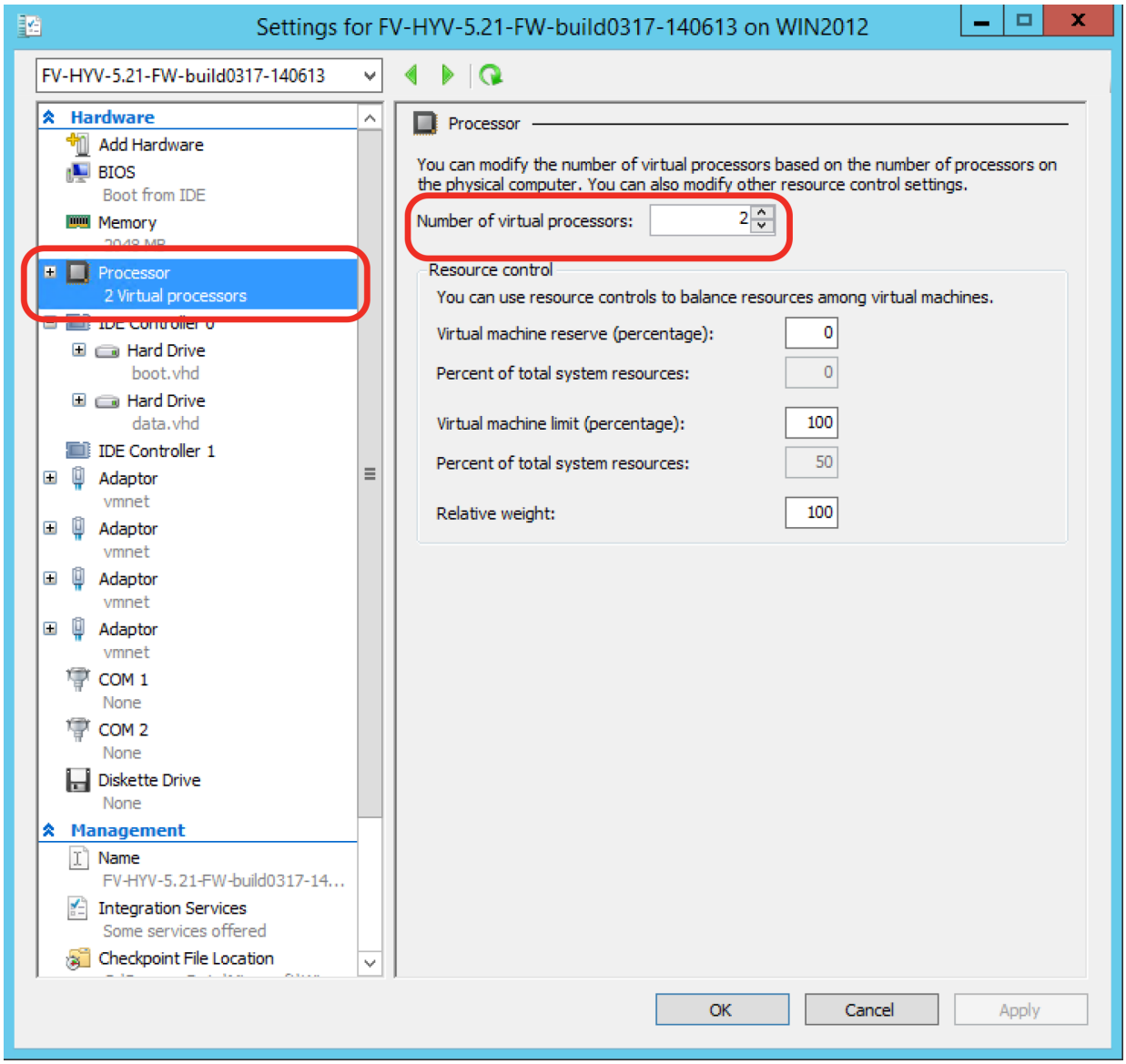
By default, the virtual appliance is configured to use 1 vCPU. Depending on the FortiWeb-VM license that you purchased, you can allocate from 1 to 10 vCPUs.

If you need to increase or decrease the vCPUs after the initial boot, shut down FortiWeb-VM, adjust the number of vCPUs, then see Updating the license for more vCPUs on page 155.

To change the number of vCPUs

You shut down FortiWeb-VM to resize the vCPU.

1. Shut down the virtual machine (**Actions > Shut Down**).
2. Select the FortiWeb-VM virtual machine in the list of machines, and then, under **Actions**, click **Settings**.
3. Under **Hardware**, select the **Processor** item, and then use the Processor settings to increase or decrease the number of vCPUs.

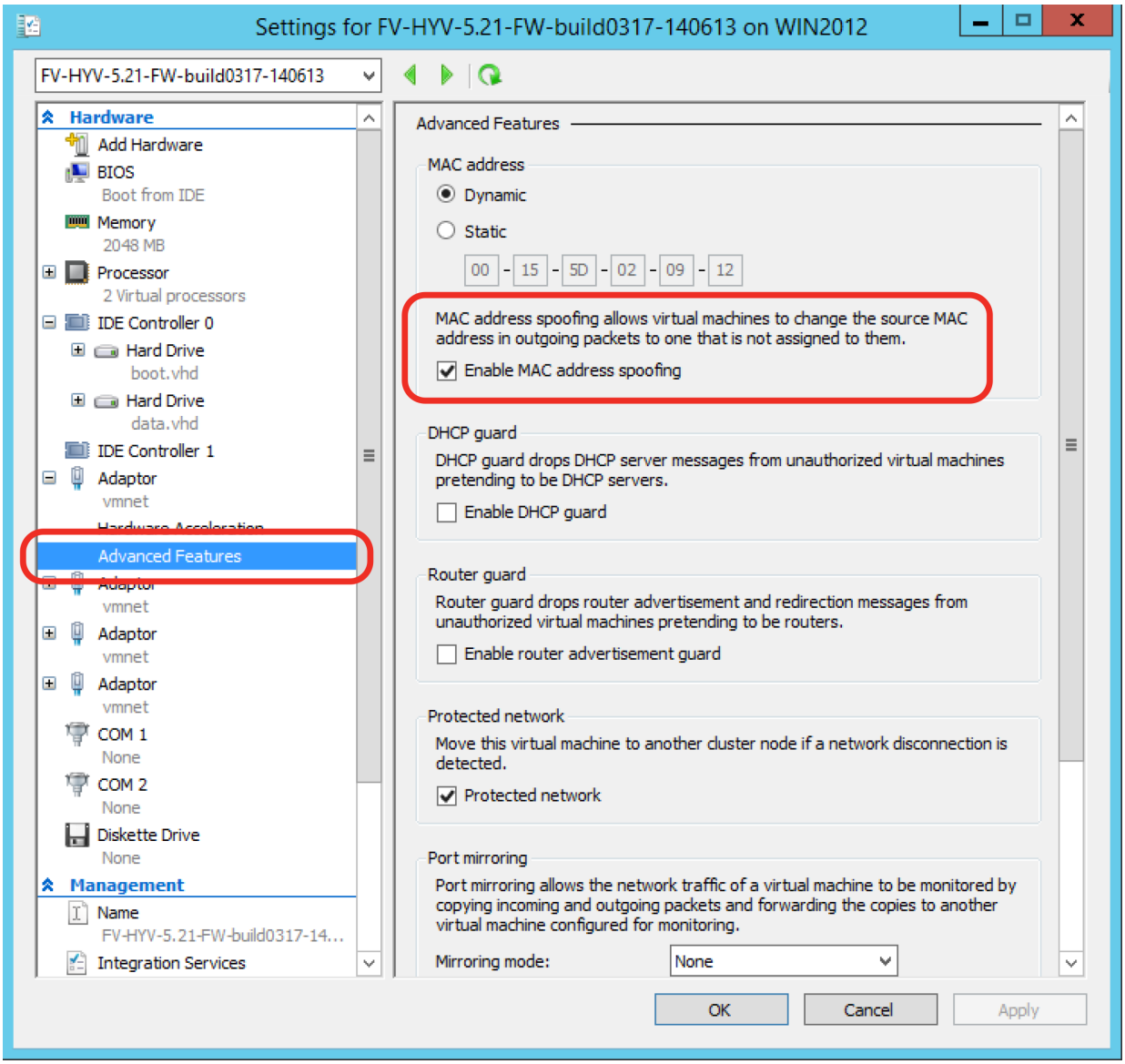


4. Click **OK** and then start the machine.

MAC address spoofing

To operate correctly, FortiWeb-VM virtual switches require MAC address spoofing. When you create a virtual switch, this option is enabled by default.

To access the option, in the settings for the virtual machine, under Hardware, expand the virtual switch item, and then select **Advanced Features**.



Mapping the virtual NICs (vNICs) to physical NICs

When you import the FortiWeb-VM package, the import process creates 4 bridging vNICs and automatically maps them to a port group on 1 virtual switch (vSwitch) within the hypervisor (the default name of this vSwitch is `vmnet`). Each of the 4 network interfaces in FortiWeb-VM uses one of these vNICs. (Alternatively, you can configure some or all of the network interfaces to use the same vNIC.) vSwitches are themselves mapped to physical ports on the server.

In many cases, you do not need to change the default mappings of the FortiWeb-VM network adapter ports to the host computer's physical ports.

You can change the mapping, or map other vNICs, if either your VM environment requires it or you want the FortiWeb-VM to operate in either true transparent proxy or transparent inspection mode. (See Configuring the vNetwork for the transparent modes on page 118.)

If you are unsure of your network mappings, try bridging before you attempt non-default vNIC modes such as NAT or host-only networks. The default bridging vNIC mappings are appropriate for configurations where each of the host's guest virtual machines have their own IP addresses on your network.

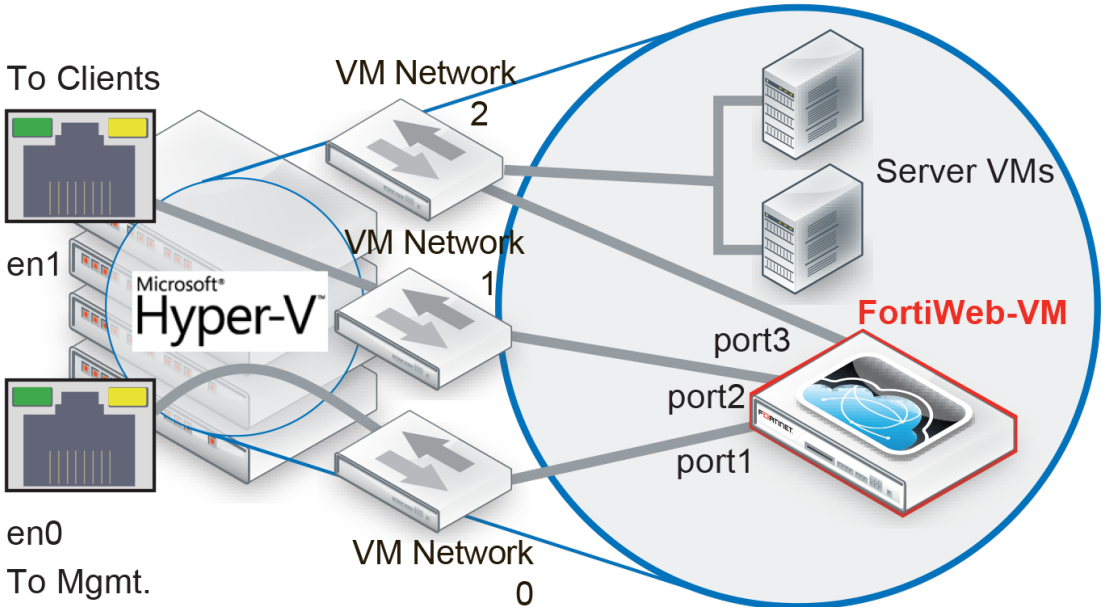
Configuring the vNetwork for the transparent modes

The default vNetwork configuration does **not** function with FortiWeb bridges (V-zones), which you use if you deploy your FortiWeb-VM in either true transparent proxy or transparent inspection operation mode.

To support the transparent modes, you **must**:

- ensure a total of at least three network cards are available to Hyper-V
- add 2 vSwitches for the bridge: one for the web server side, and one for the client side
- map the new vSwitches to a network adapter (vNIC)

Similar to a deployment that does not use virtual machines, connections between clients and servers are piped through the two vSwitches that comprise the bridge, with FortiWeb-VM in between them.



To create a vSwitch

1. In the Hyper-V Manager, under **Actions**, click **Virtual Switch Manager**.
2. Under **Virtual Switches**, click **New virtual network switch**, click **External**, and then click **Create Virtual Switch**.
3. Under **Virtual Switch Properties**, for **Name**, enter a network label that identifies the port group.

   For example, `Client-Side-vSwitch1`.

   For all other settings, use the default values.
4. Click **OK**.
5. Repeat this procedure to create the other vSwitch.

   For example, create a vSwitch with the name `Server-Side-vSwitch2`.

6. In the list of virtual machines, select the FortiWeb-VM machine, and then click **Settings**.
7. Under Hardware, for the second and third **Adaptor** items, select the virtual switches you created earlier.

   For example, select `Client-Side-vSwitch1` and `Server-Side-vSwitch2`.
8. Click **OK**.
9. Later, when you configure FortiWeb-VM, add port2 and port3 (or whichever FortiWeb ports correspond to the vSwitches you created in this procedure) to the bridge (V-zone).

Start the FortiWeb-VM

You can now power on your FortiWeb-VM. Select the name of the FortiWeb-VM in the list of virtual machines, right-click, and select **Start** in the menu. Optionally, you can select the name of the FortiWeb-VM in the list of virtual machines and select **Start** in the **Actions** menu.

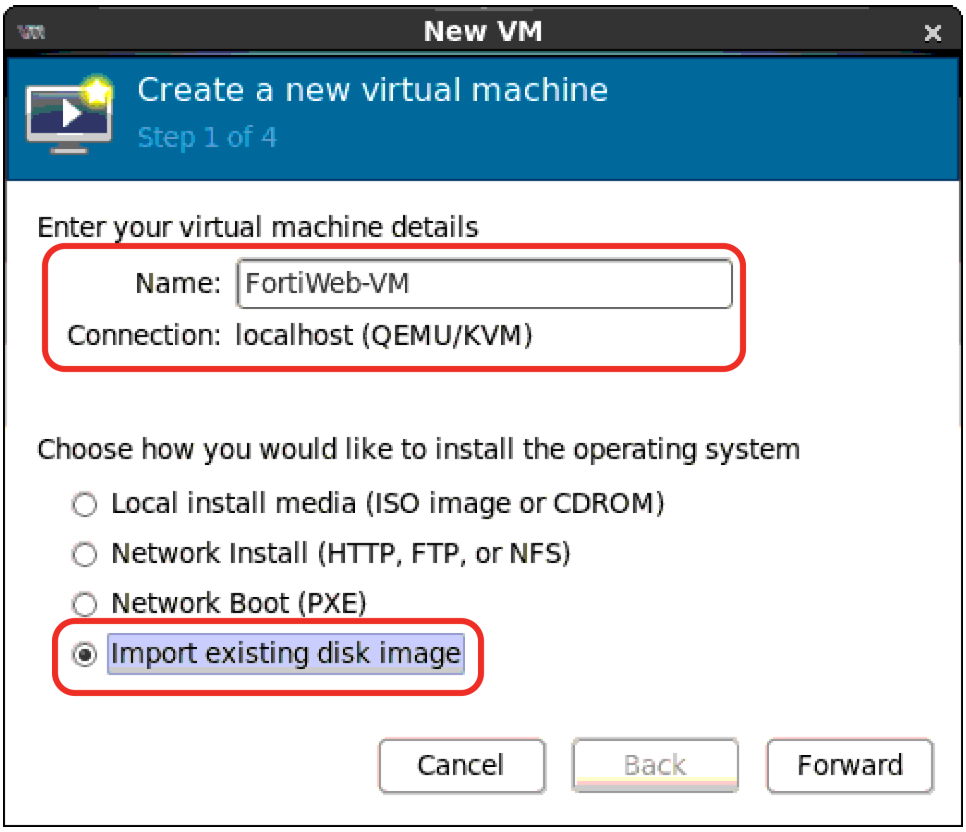
Deploying FortiWeb-VM on KVM

You deploy FortiWeb-VM on KVM (for Kernel-based Virtual Machine) by importing a disk image.

Import the FortiWeb-VM virtual machine

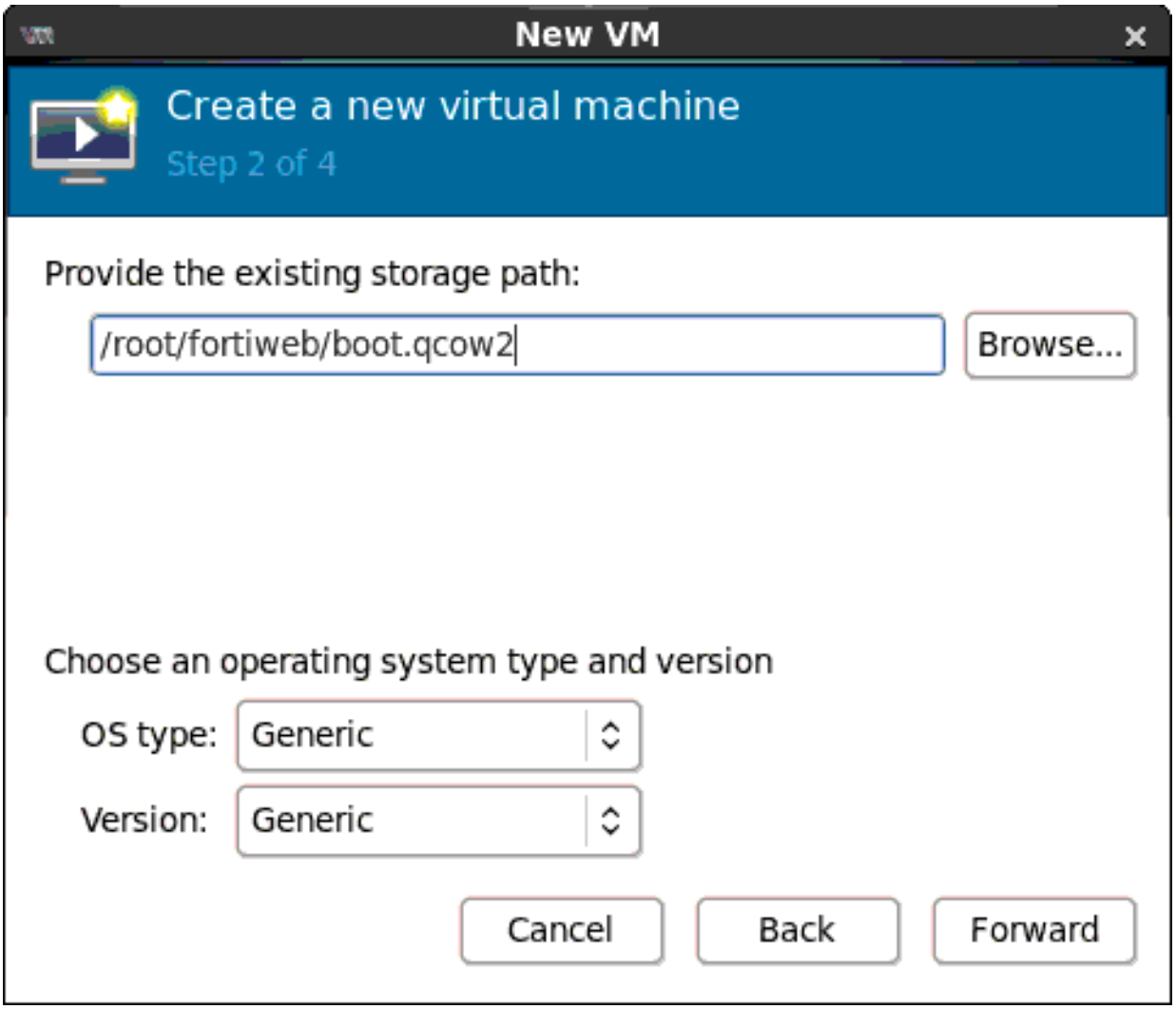
To import the FortiWeb-VM virtual machine

1. Obtain the FortiWeb-VM installation files using the instructions provided in Downloading the FortiWeb-VM software on page 18.
2. On your KVM host server, launch Virtual Machine Manager (virt-manager), and then select **Create a new virtual machine**.
3. Enter a name for the VM (for example, `FortiWeb-VM`).
4. Ensure that **Connection** is **localhost** (the default value).
5. Select **Import existing disk image**.



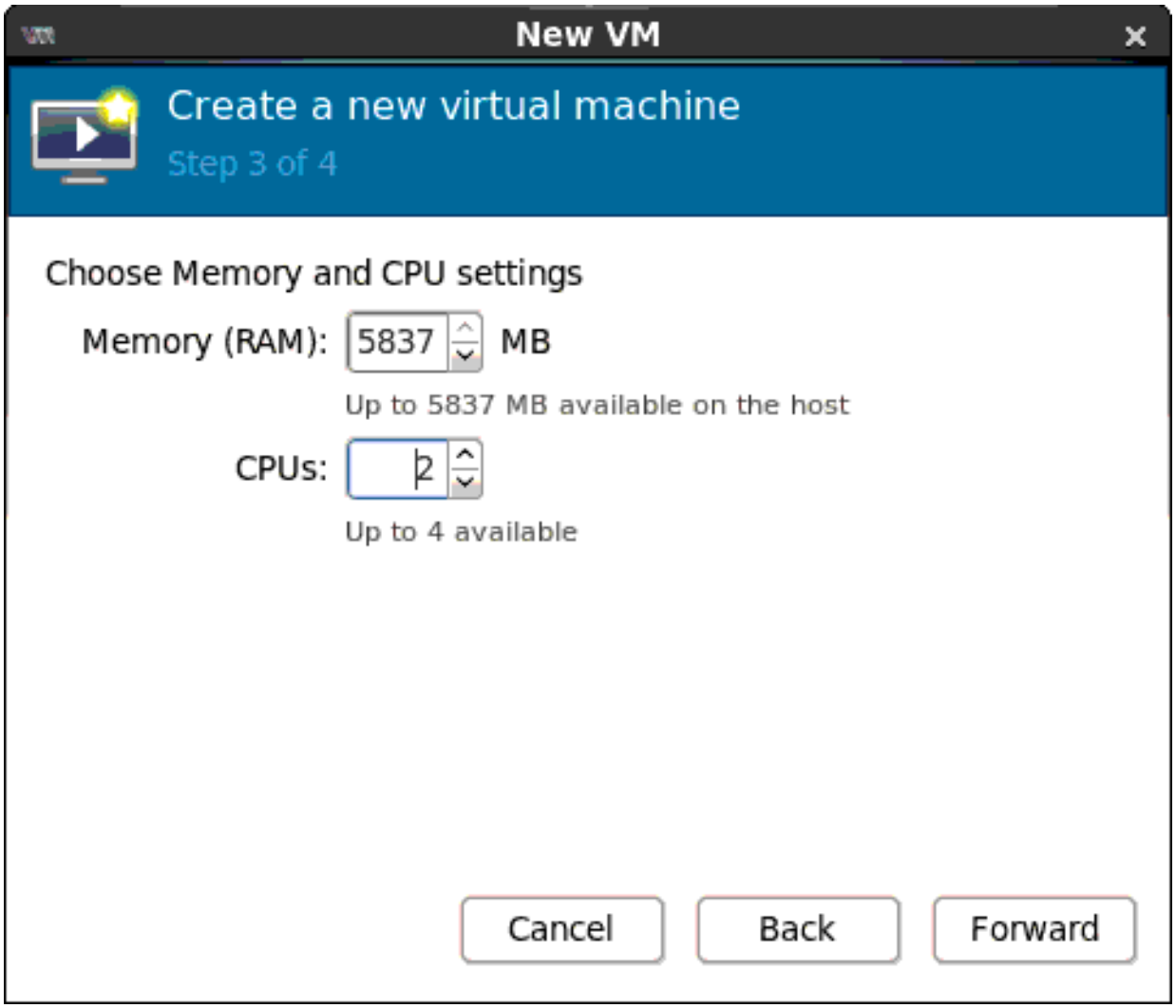
6. Click **Forward**.
7. Click **Browse** to navigate to `boot.qcow2` and select it.

8. Use the default values for **OS Type** and **Version**.



9. Click **Forward**.
10. Specify the amount of memory and number of CPUs to allocate to this virtual machine.

Ensure the values do not exceed the maximums for your license.

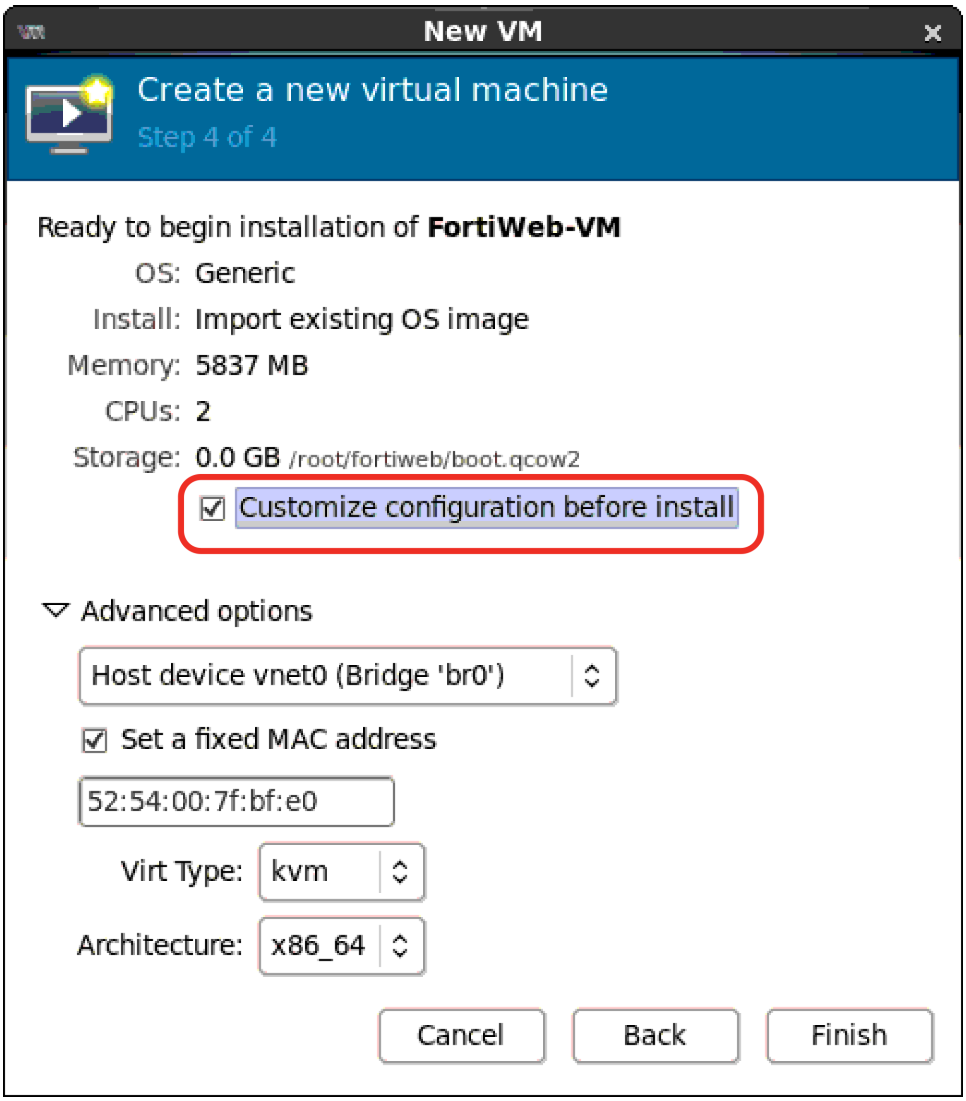


It is possible to configure FortiWeb-VM to use less vRAM, such as 2 GB. However, for performance reasons, Fortinet recommends that you use at least 4 GB.

For example, if you use only 1 GB of vRAM, FortiWeb-VM cannot update its FortiGuard protection feature when **Extended Virus Database** is selected. (You can still update the service using the **Regular Virus Database** option.)

11. Click **Forward**.

12. Select **Customize configuration before install**.



13. Click **Finish**.

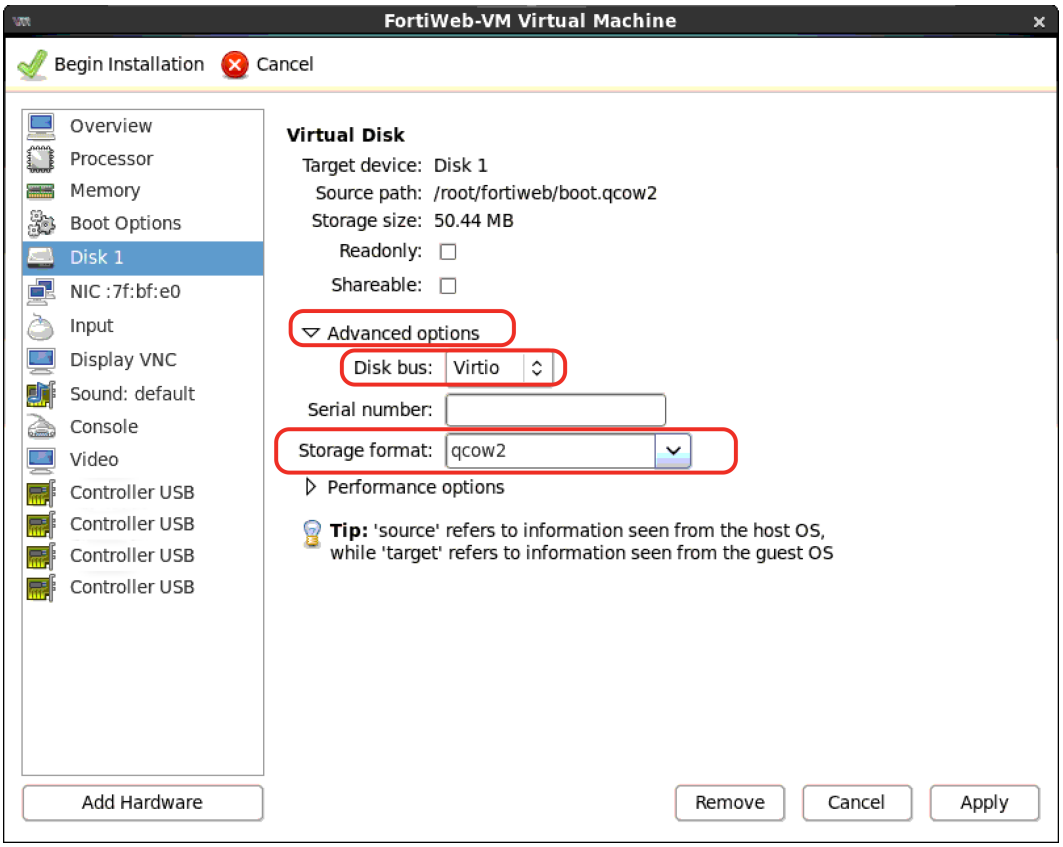
14. Optionally, to add a serial device, click **Add Hardware**, and then do the following:

- Ensure **Serial** is selected.
- For **Device type**, select **TCP network console(tcp)**.
- For **Mode**, select **Server mode(bind)**
- For **Host**, enter `127.0.0.1`.
- For **Port**, enter `10301`.
- Click **Finish**.

This serial device allows you to connect to the CLI. Once you have a CLI connection, you can perform the basic configuration that allows you to connect to the web UI to complete your configuration tasks, or complete your configuration using the CLI only. Otherwise, use the instructions in Configuring access to FortiWeb's web UI & CLI on page 143

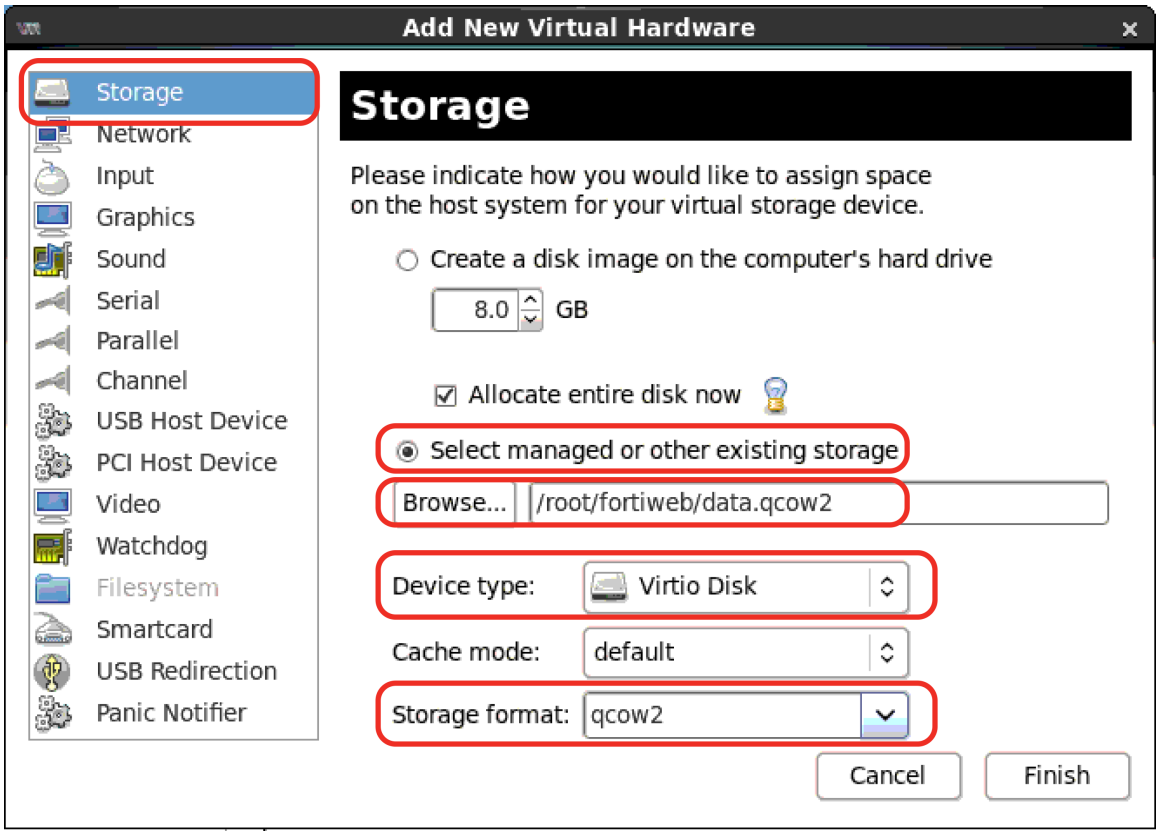
15. Select the virtual disk to display its properties.

16. Under **Advanced options**, for **Disk bus**, select **Virtio**, and for **Storage format**, select **qcow2**.



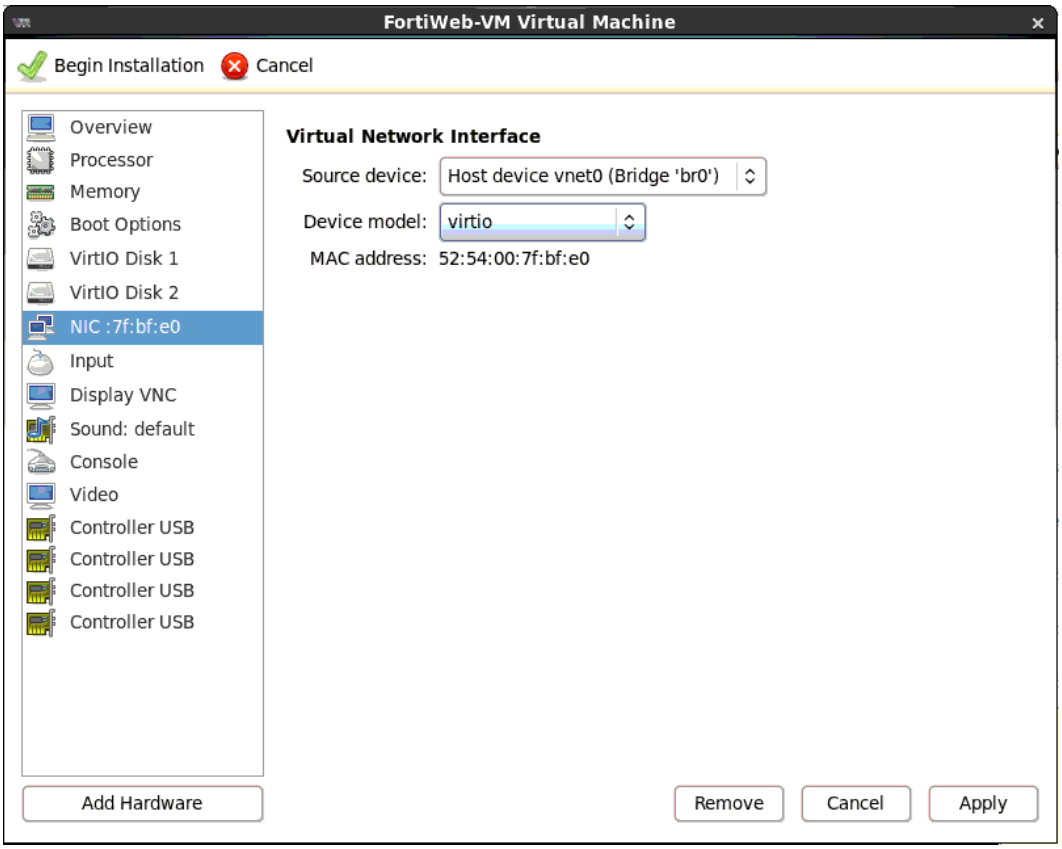
17. Select **Apply**.
18. To add a new virtual storage device, click **Add Hardware**.
19. Do the following:
    - Ensure **Storage** is selected.
    - Select **Select managed or other existing storage**.
    - Click **Browse** to navigate to `data.qcow2` and select it.
    - For **Device type**, select **Virtio disk**.

- For **Storage format**, select **qcow2**.



20. Click **Finish**.

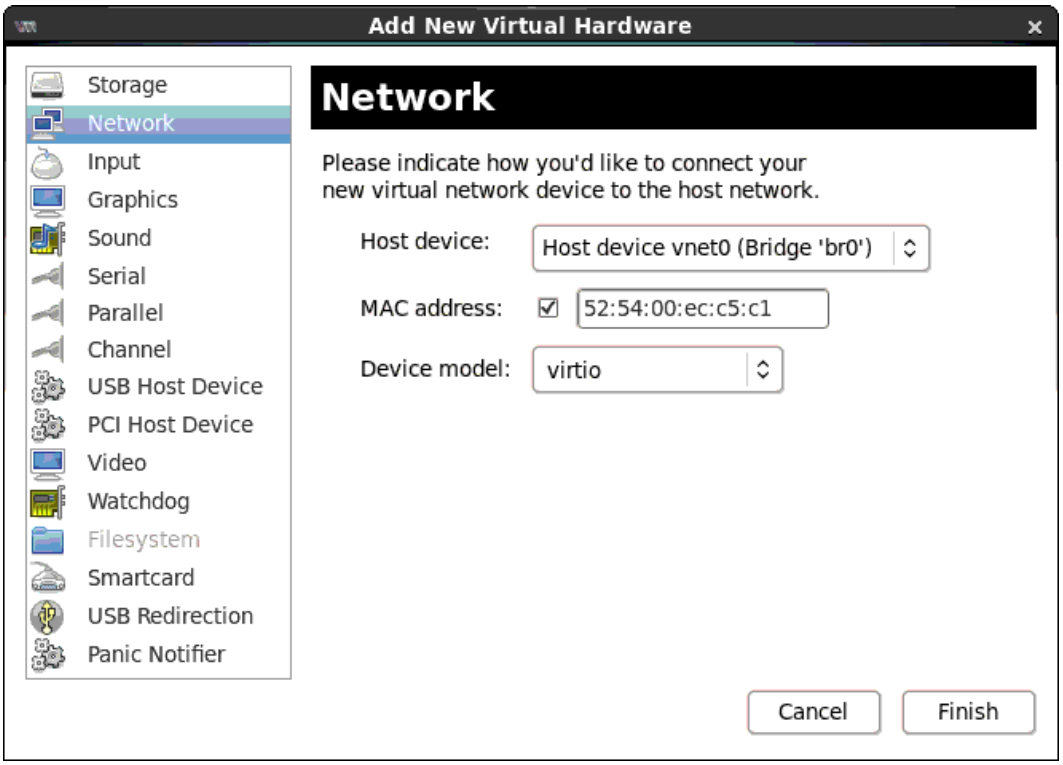
21. Select the virtual network interface (vNIC) and change its type to **virtio**.



22. Click **Apply**.

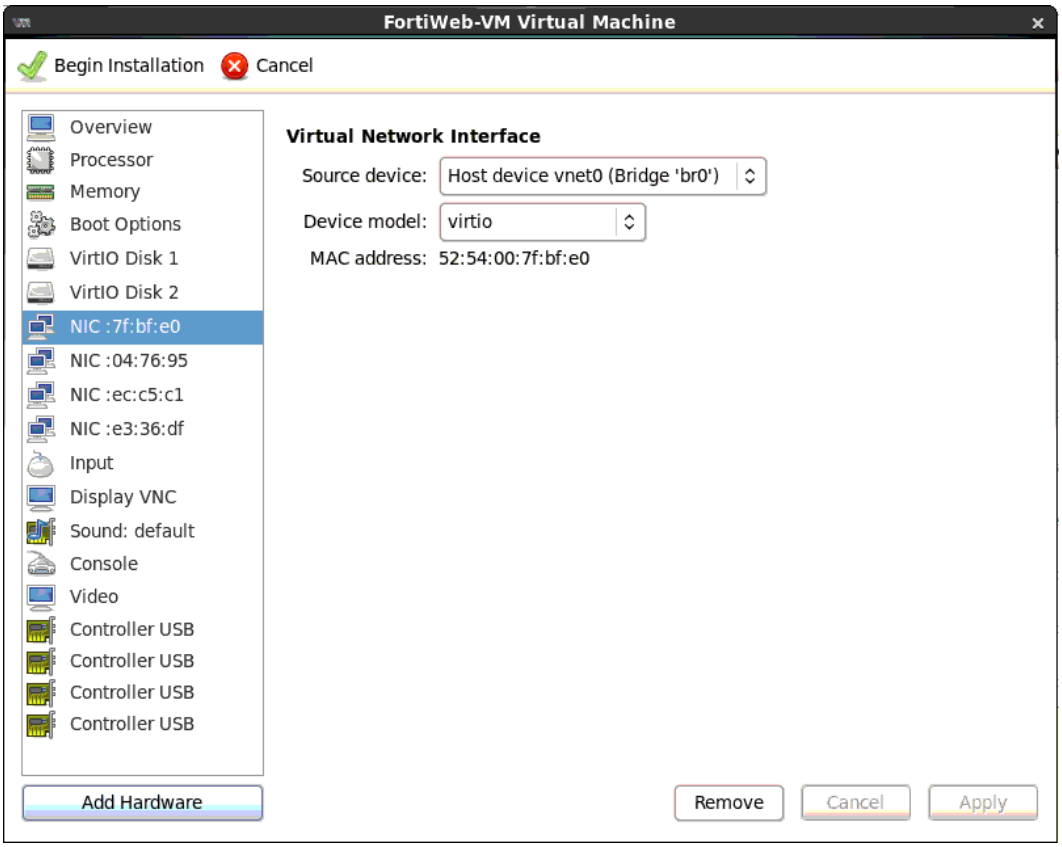
23. To add an additional vNIC, first click **Add Hardware**, and then click **Network**.

24. For device model, select **vitrio**.



25. Click **Finish**.

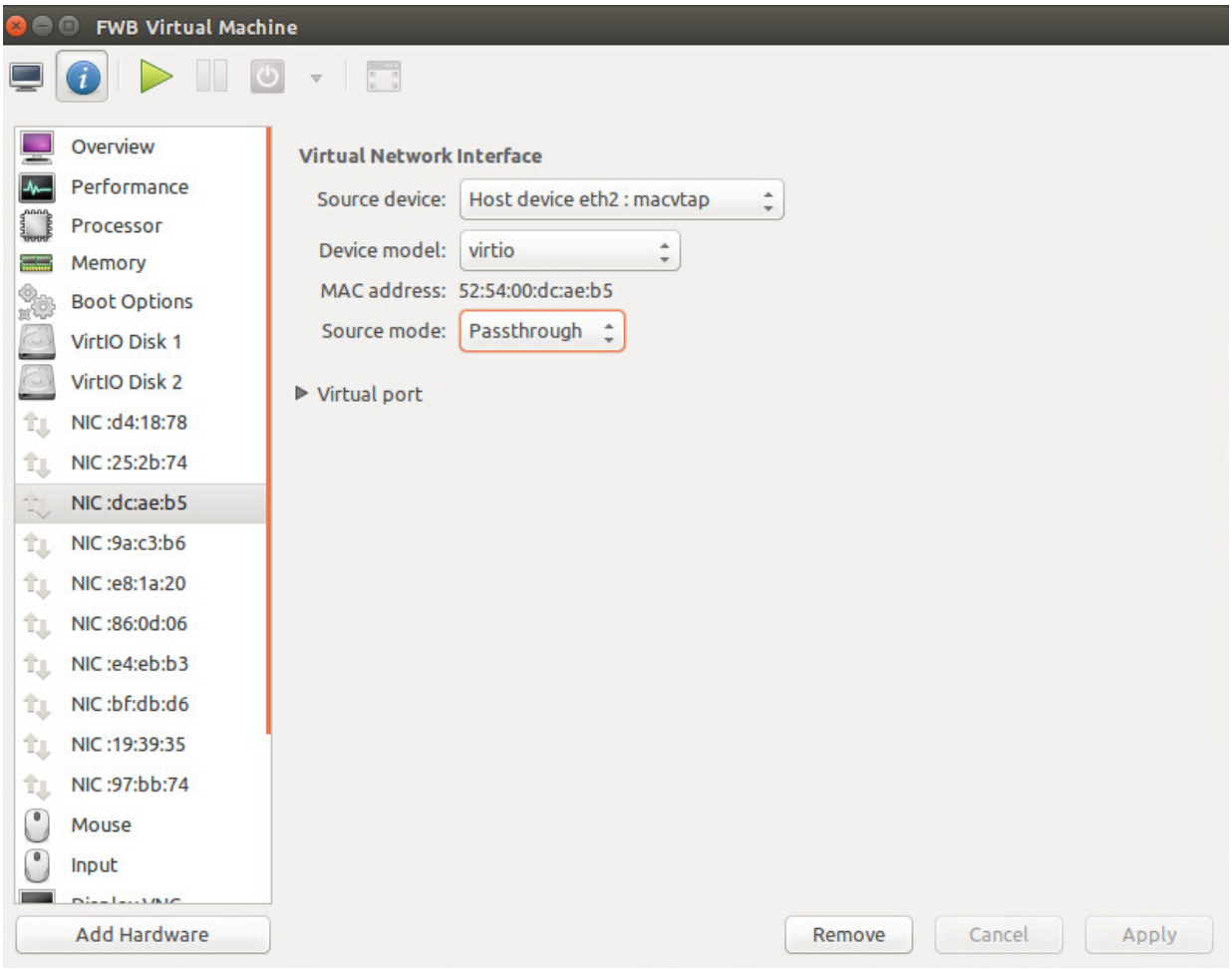
26. Use the vNIC creation steps to add two additional virtio vNICs.



27. Click **Begin Installation**.

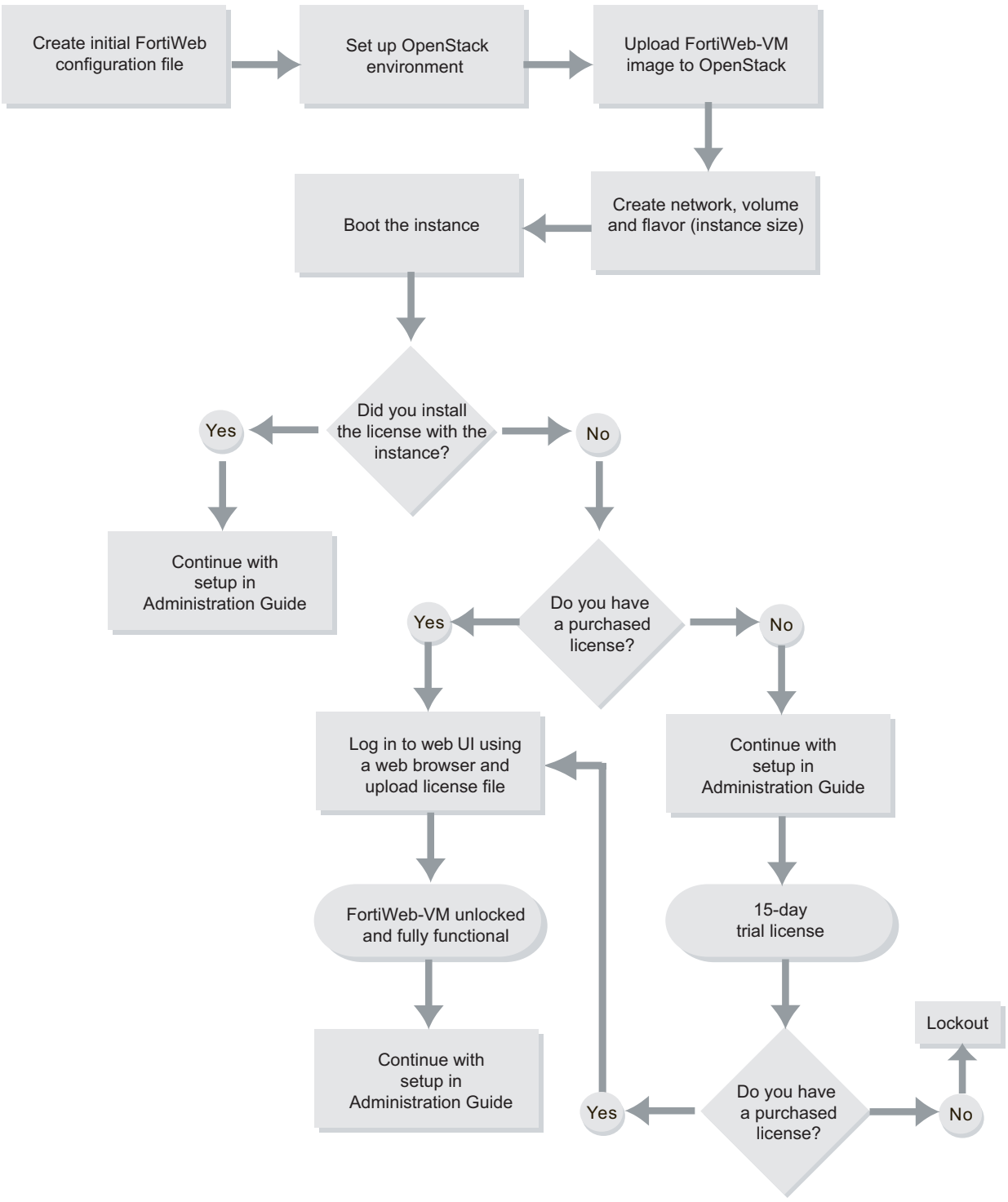
Configuring the vNICs for transparent modes

To allow FortiWeb-VM deployed on KVM to work in true transparent proxy or transparent inspection operation mode, set the source mode for the the virtual network interfaces to **Passthrough**. This configuration allows the interfaces to work with FortiWeb bridges (V-zones).


FWB Virtual Machine
Overview
Performance
Processor
Memory
Boot Options
VirtIO Disk 1
VirtIO Disk 2
NIC :d4:18:78
NIC :25:2b:74
NIC :dc:ae:b5
NIC :9a:c3:b6
NIC :e8:1a:20
NIC :86:0d:06
NIC :e4:eb:b3
NIC :bf:db:d6
NIC :19:39:35
NIC :97:bb:74
Mouse
Input
Add Hardware
Virtual Network Interface
Source device: Host device eth2 : macvtap
Device model: virtio
MAC address: 52:54:00:dc:ae:b5
Source mode: Passthrough
Virtual port
Remove
Cancel
Apply

Deploying FortiWeb-VM on OpenStack

You deploy FortiWeb-VM on the OpenStack cloud computing platform using the KVM version of the FortiWeb-VM software.



Preparing to deploy on OpenStack

Download the FortiWeb-VM license and software

You can include the license file when you deploy FortiWeb-VM on OpenStack. See Downloading the FortiWeb-VM license & registering with Technical Support on page 17.

If you do not include the license file, the instance runs using the built-in trial license and you can upload the license later. For more information, see Licensing on page 7.

Download the appropriate KVM version of the FortiWeb-VM software and extract the `.zip` compressed archive's contents. The archive's contents include the image file `boot.qcow2` that you upload to OpenStack.

For more information, see Downloading the FortiWeb-VM software on page 18.

Creating an initial FortiWeb configuration file

Deploying a FortiWeb-VM instance on OpenStack requires a FortiWeb configuration file.

Ensure the file configures:

- port1 to use DHCP, which allows it to acquire an IP address from OpenStack
- A DNS server address for verifying the FortiWeb-VM license

You can include additional configuration that takes affect when you deploy the FortiWeb-VM instance.

The following commands are an example of the configuration file:

```
config system global
set hostname KVM-CLOUD-INIT
set admintimeout 480
end
config system interface
edit "port1"
set type physical
set allowaccess https ping ssh snmp http telnet
set mode dhcp
config secondaryip
end
next
end
config system dns
set secondary 114.114.114.114
end
```

Deploying FortiWeb-VM on OpenStack

The examples shown in this procedure create a FortiWeb-VM instance with the following properties:

- A direct connection to the public network
- A 30GB log disk (an OpenStack volume)

- 2 vCPUs with 2GB RAM and a 2GB root disk (specified by the OpenStack flavor)
- Fully licensed

1. To set up your OpenStack environment, create an `openrc.sh` (OpenStack rc) file that specifies the admin credentials and admin endpoint.

   For example, the OpenStack rc file `admin-openrc.sh` has the following is the content:

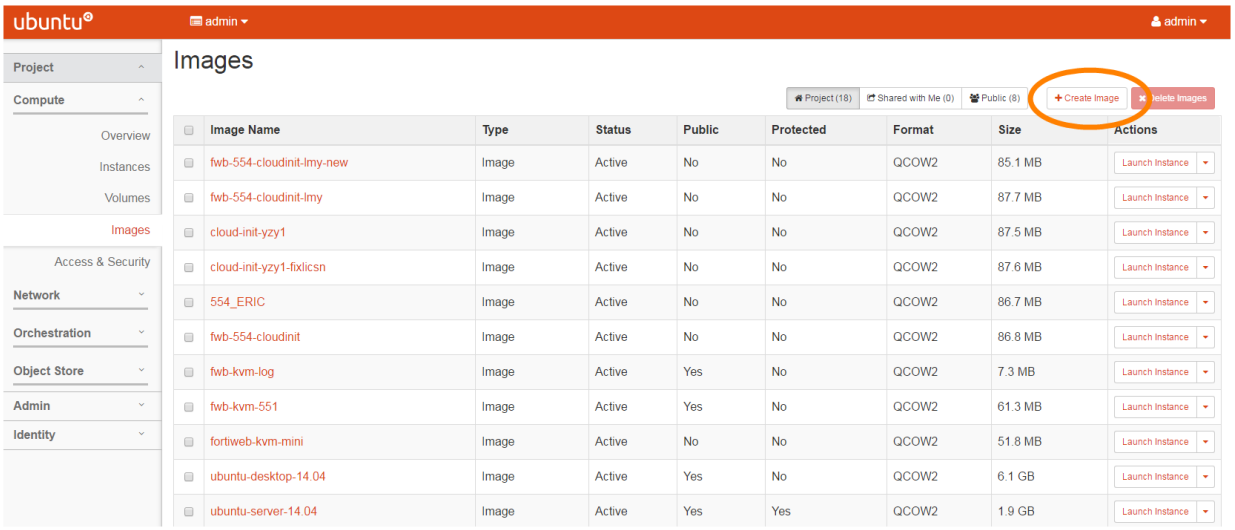
```
openstack@controller:~$
openstack@controller:~$ cat admin-openrc.sh
export OS_PROJECT_DOMAIN_ID=default
export OS_USER_DOMAIN_ID=default
export OS_PROJECT_NAME=admin
export OS_TENANT_NAME=admin
export OS_USERNAME=admin
export OS_PASSWORD=fortiweb
export OS_AUTH_URL=http://controller:35357/v3
export OS_IDENTITY_API_VERSION=3

export HEAT_DOMAIN_PASSWORD=fortiweb
export OS_IMAGE_API_VERSION=2
export OS_AUTH_VERSION=3
#export OS_TOKEN=7e6bb6afe0d80196e240
#export OS_URL=http://10.200.2.120:35357/v2.0/
#export SERVICE_TOKEN=7e6bb6afe0d80196e240
openstack@controller:~$
```

2. Using the shell you use to run OpenStack commands, source the OpenStack rc file. For example:

   ```
   $ source admin-openrc.sh
   ```

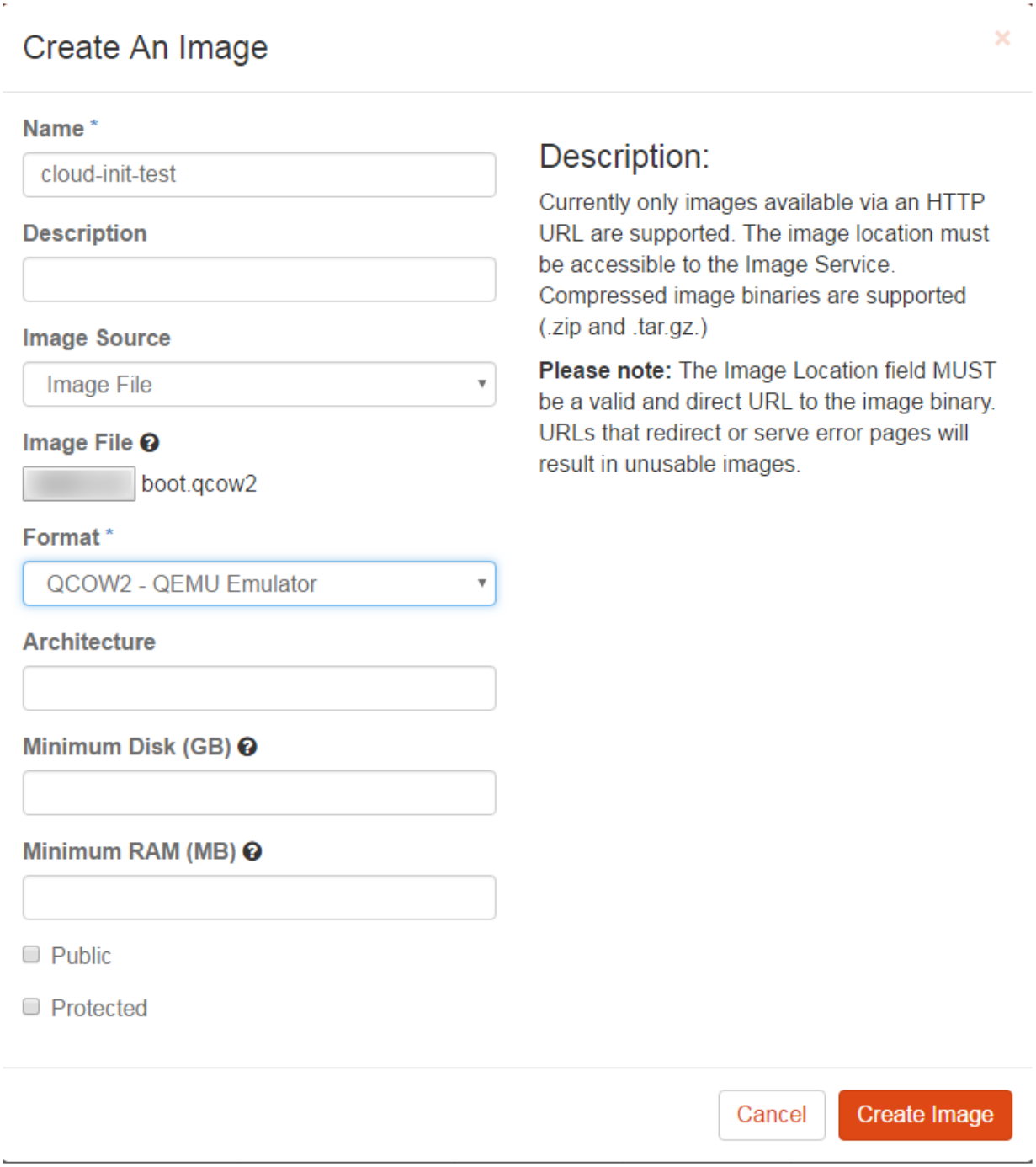
3. Log in to the OpenStack dashboard, under **Compute**, navigate to the list of images, and then click **Create Image**.



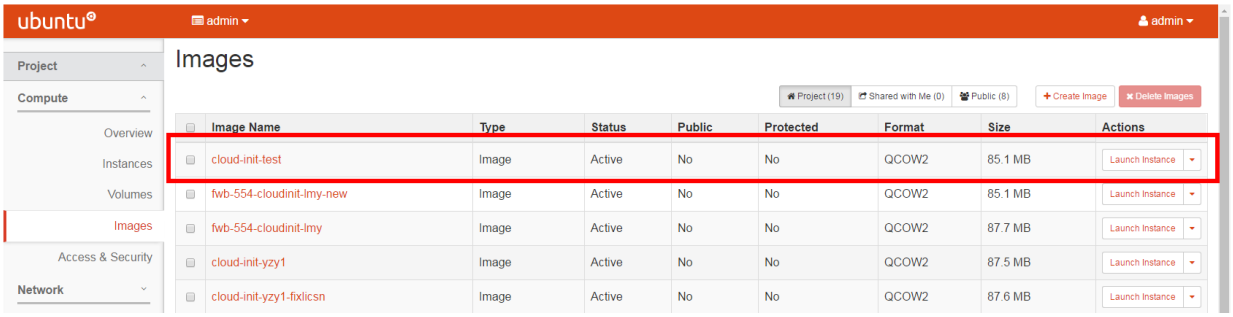
4. Complete the image settings.

   For **Image Source**, select **Image File**. Use the Image File options to navigate to and select the `boot.qcow2` file you extracted from the FortiWeb-VM KVM software package. For **Format**, select

QCOW2-QEMU Emulator.



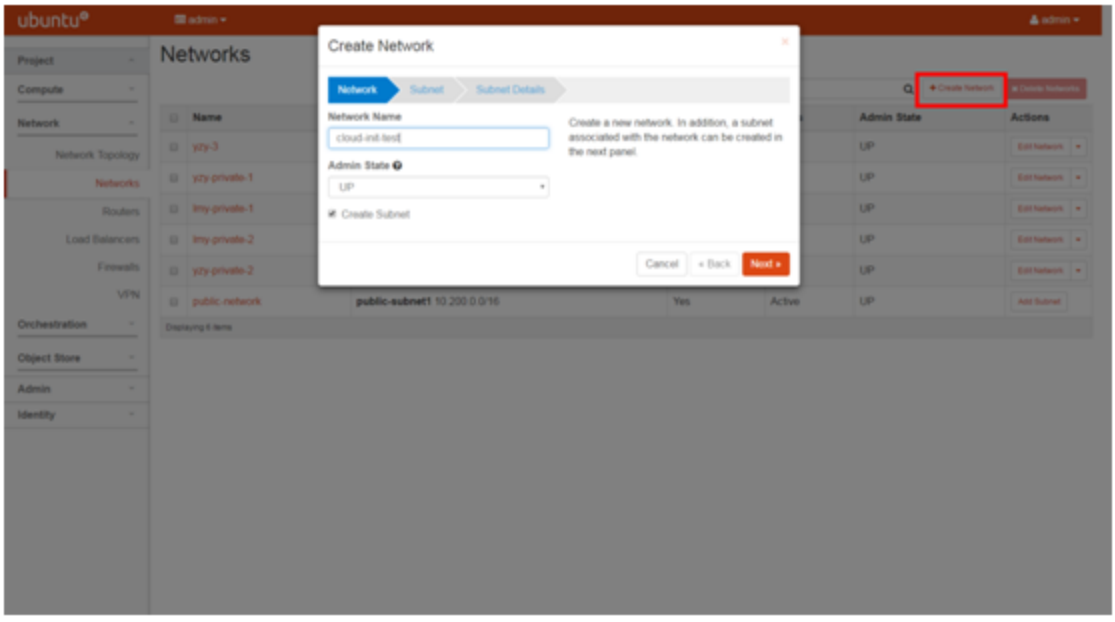
5. Click **Create Image**, and then use the dashboard to verify that OpenStack added the image.

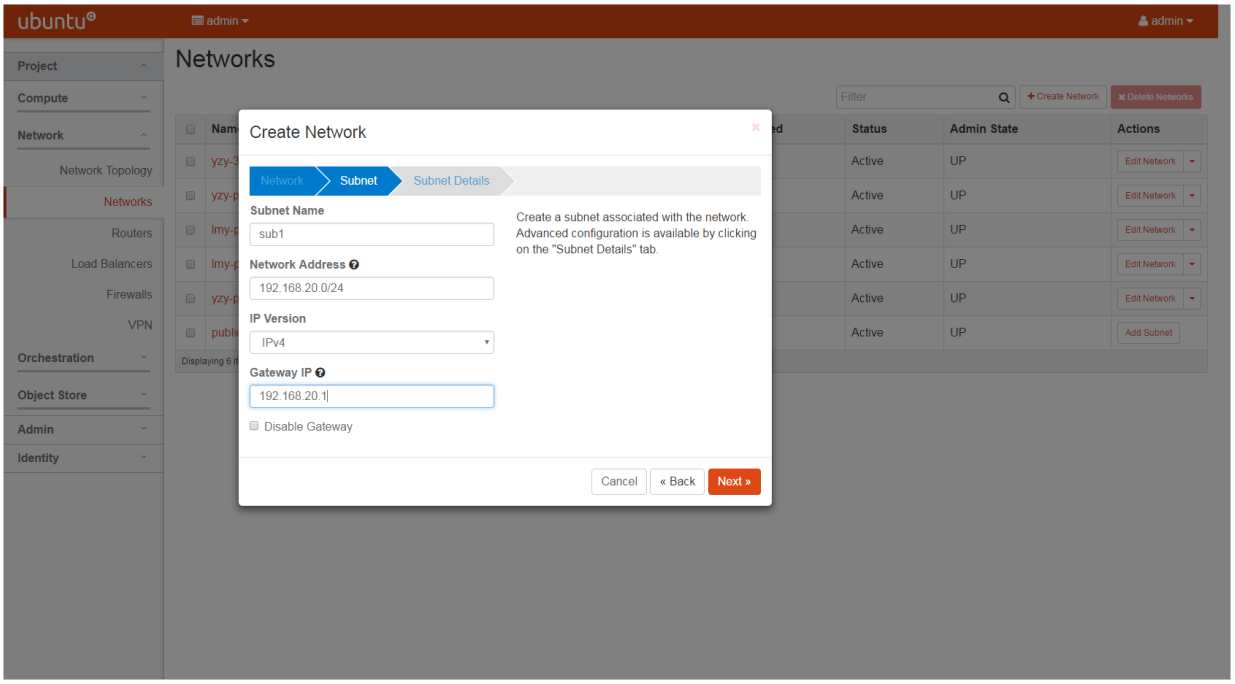


Alternatively, use the CLI command `nova image-list` to verify the image.

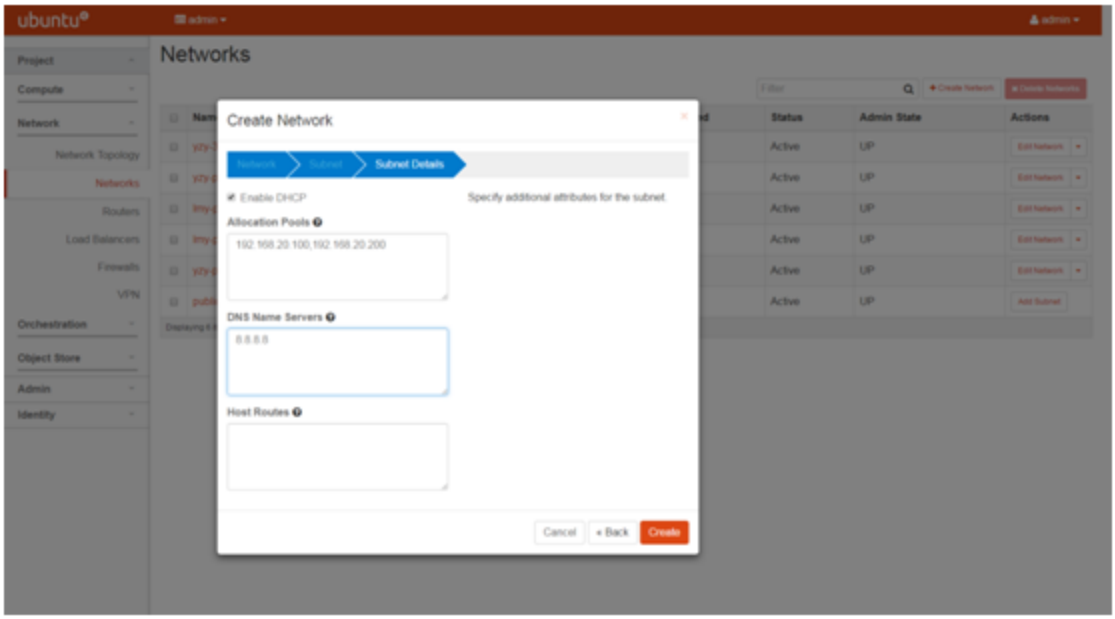
```
openstack@controller:~$ source admin-openrc.sh
openstack@controller:~$
openstack@controller:~$
openstack@controller:~$ nova image-list
+--------------------------------------+---------------------------+--------+--------------------------------------+
| ID                                   | Name                      | Status | Server                               |
+--------------------------------------+---------------------------+--------+--------------------------------------+
| 70295811-84b2-4544-9771-a1a60868ae53 | 554_ERIC                  | ACTIVE |                                      |
| 81e4b49f-81d2-4201-b7c0-8de4a1033750 | cirros                    | ACTIVE |                                      |
| 9c5f1433-0c64-4aa9-9461-d961a5eabe87 | cloud-init-test           | ACTIVE |                                      |
| 4c52834b-2471-490d-a31b-f033e8b660b4 | cloud-init-yzy1           | ACTIVE |                                      |
| 7f35bf8c-8e7b-4da6-9ab8-f46e153336a2 | cloud-init-yzy1-fixlicsn  | ACTIVE |                                      |
| 36da57d2-c2fe-4b1a-b519-f4bc08b586ac | debian8                   | ACTIVE |                                      |
| 7ab60dd0-cfa4-4613-a2fb-ceffa64a8b2b | eric_FWBlog               | ACTIVE |                                      |
| 4c7f864a-f3f5-4134-a207-edb3438b3296 | fortiweb-kvm              | ACTIVE |                                      |
| 3c84faaa-e46d-41b7-9ffd-d746a61ce724 | fortiweb-kvm-mini         | ACTIVE |                                      |
| a4055563-a40a-4df2-9230-a3435ef4b80e | fwb-554-cloudinit         | ACTIVE |                                      |
| 74610607-1088-4d12-afb7-ae0c3a0251d6 | fwb-554-cloudinit-lmy     | ACTIVE |                                      |
| fc113caa-0047-4d93-91c6-bd24561cb356 | fwb-554-cloudinit-lmy-new | ACTIVE |                                      |
| 2f61765a-fcb7-41e7-bba0-68dd49d6519a | fwb-kvm-551               | ACTIVE |                                      |
| c653f21a-c5e4-41f0-a11a-eed631a7ec77 | fwb-kvm-log               | ACTIVE |                                      |
| ebe8ab34-60d6-4525-8cd4-f4a15c91e0c0 | ubuntu-desktop-14.04      | ACTIVE |                                      |
| 3e41de51-a74b-4f3c-aef6-d57bc21e5b01 | ubuntu-server-14.04       | ACTIVE |                                      |
| 0ed61f12-e2b2-48a9-a478-ffc7d1e4fa65 | yzy-log-disk              | ACTIVE |                                      |
| ee9cfc59-01e2-4e09-8709-a0a34afff999 | zg-boot                   | ACTIVE |                                      |
| b7ee658c-c337-423b-8d95-dd5460764d7f | zg-snapshot1              | ACTIVE | dc5abe2e-799b-47a3-b94b-03d31b755621 |
+--------------------------------------+---------------------------+--------+--------------------------------------+
openstack@controller:~$
```

6. In the OpenStack dashboard, navigate to the Network options and click **Create Network**.
7. In the network creation wizard, complete the network and subnet settings.

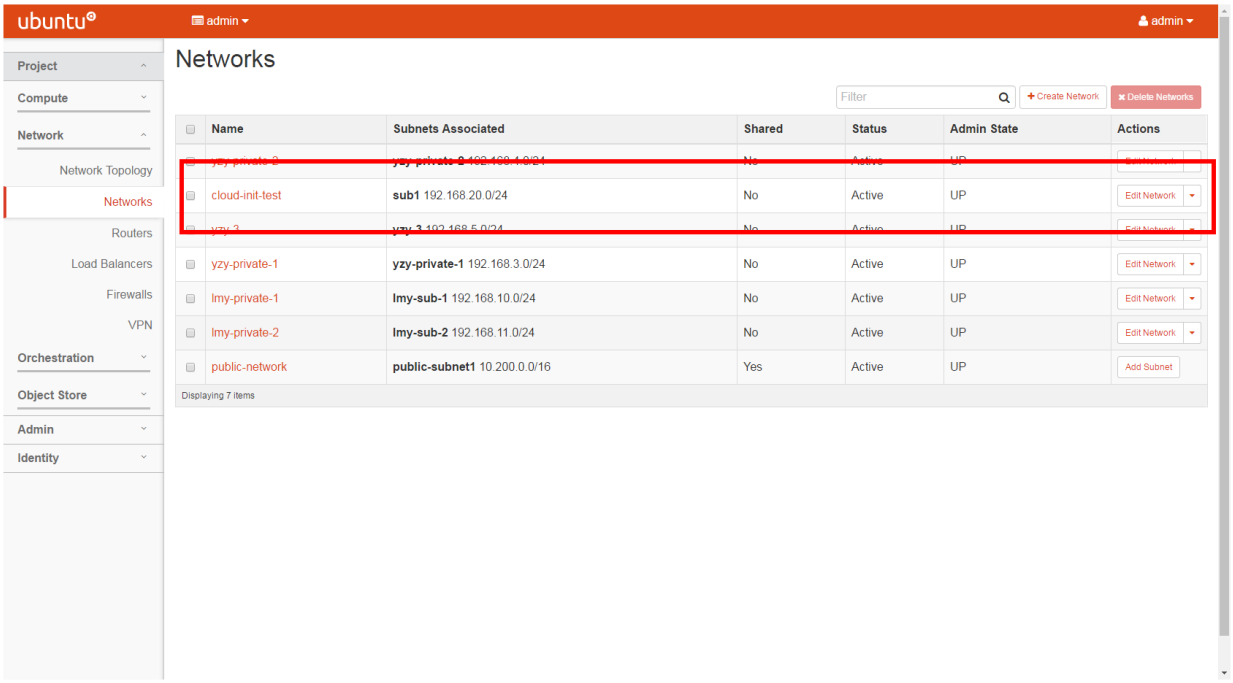




8. In the wizard, complete the subnet details. You can use a pool to assign the network's IP address range.



9. Click **Create**, and then use the dashboard to verify that OpenStack added the network.

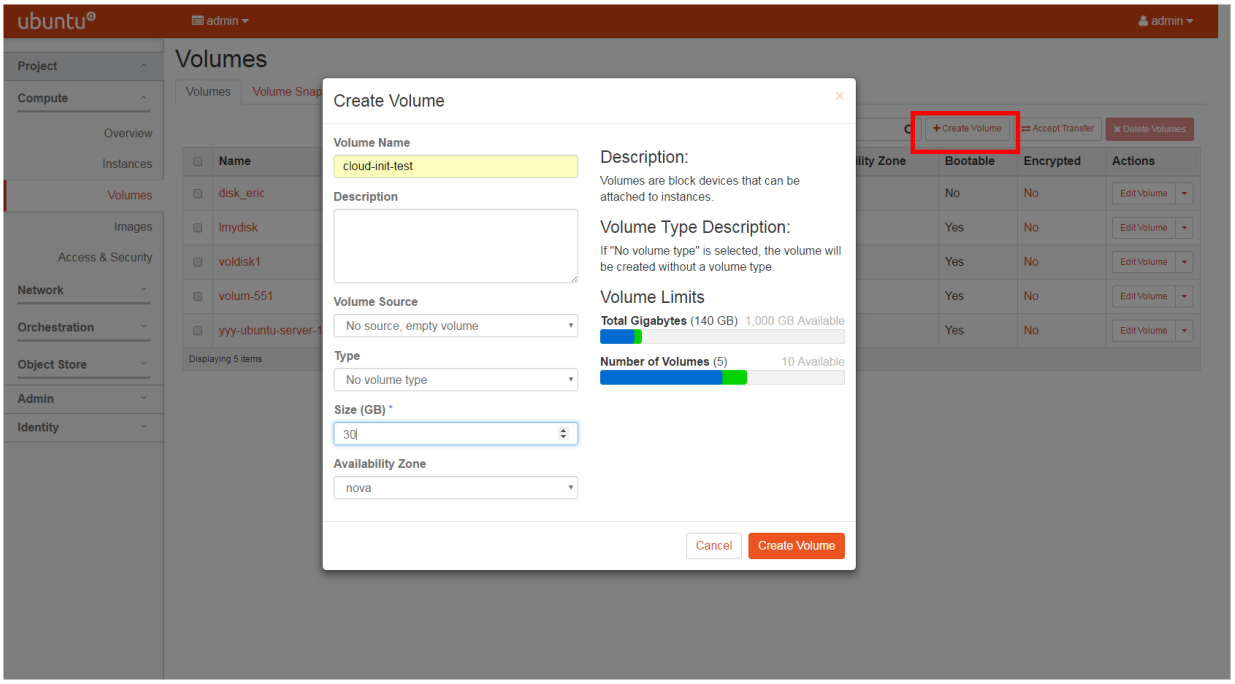


Alternatively, use the CLI command `nova network-list` to verify the image.

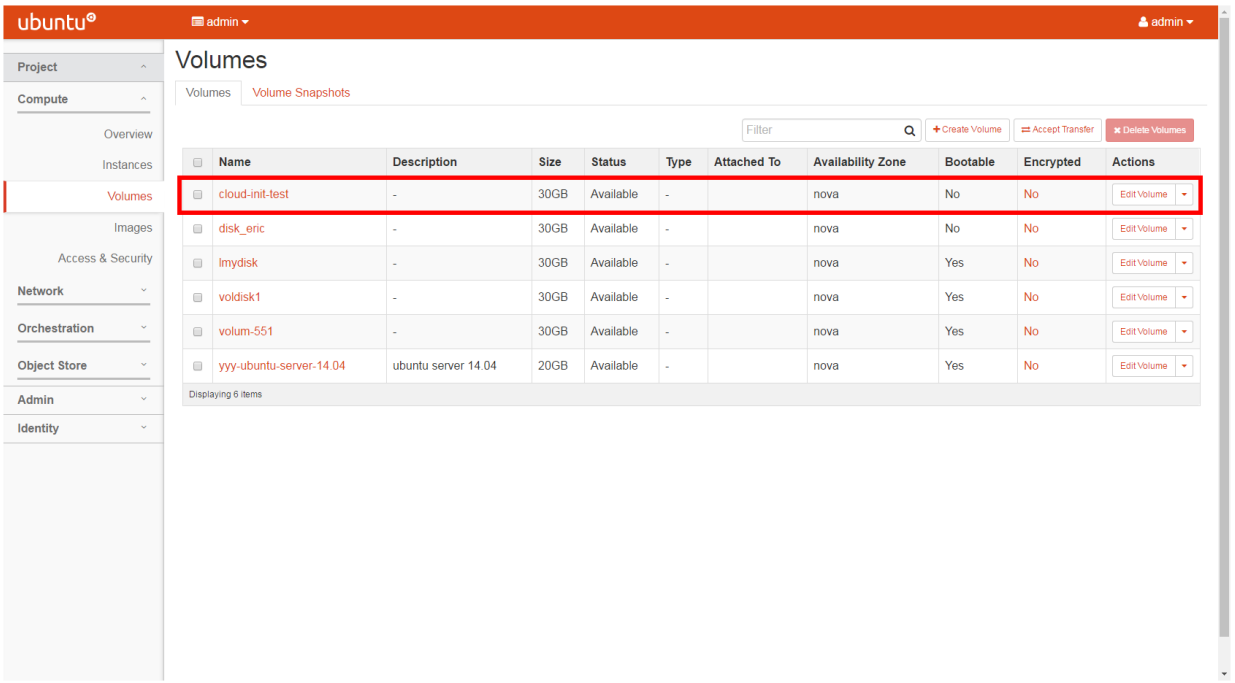
```
openstack@controller:~$ source admin-openrc.sh
openstack@controller:~$ nova network-list
+--------------------------------------+-----------------+------+
| ID                                   | Label           | Cidr |
+--------------------------------------+-----------------+------+
| 1146eb20-8828-45d3-a8a2-622276d344e4 | public-network  | -    |
| 228167fc-31ee-4fc2-b63f-3e2b3ce65ae4 | cloud-init-test | -    |
| b37585fb-ccdd-42d7-b5f2-75dca45c412b | yzy-3           | -    |
| 3ddd0ab0-8d75-41f2-bc3a-b960ec3e135d | yzy-private-1   | -    |
| 5e217877-e8db-496b-ad54-1bb454a0f1db | lmy-private-1   | -    |
+--------------------------------------+-----------------+------+
openstack@controller:~$
```

10. To create the volume FortiWeb-VM uses for its log disk, in the OpenStack dashboard, under **Compute**, navigate to the Volumes options and click **Create Volume**.

11. Complete the volume settings.



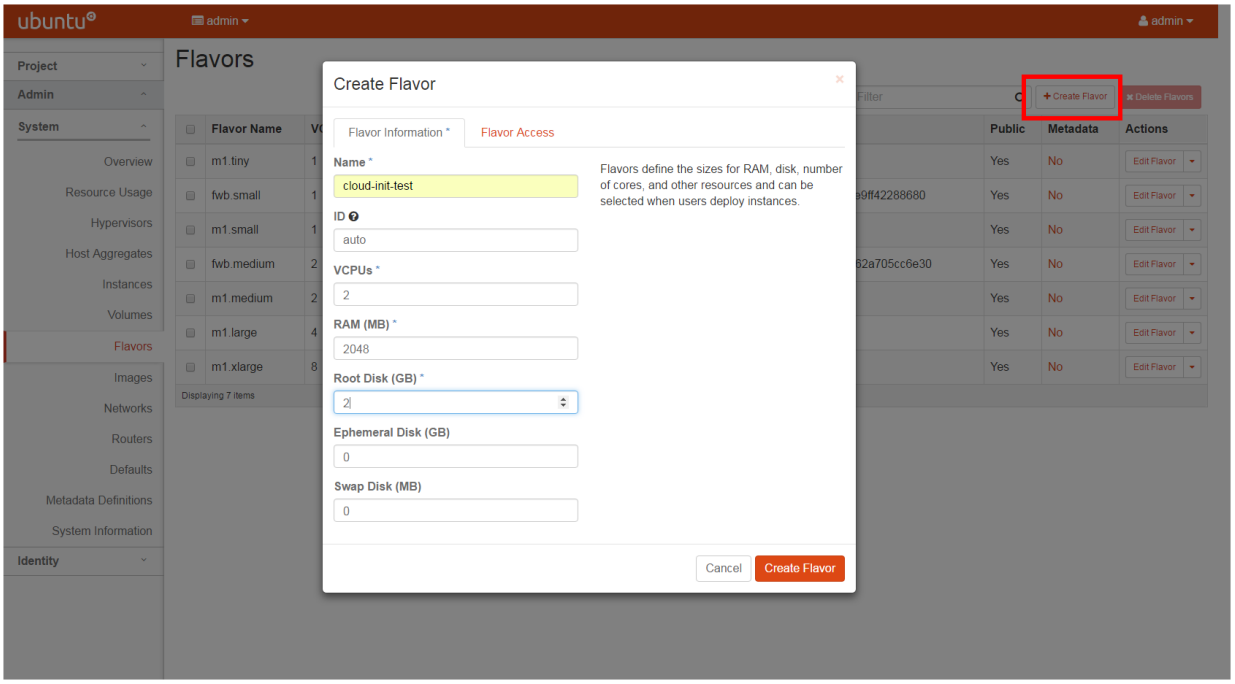
12. Click **Create Volume**, and then use the dashboard to verify that OpenStack added the volume.



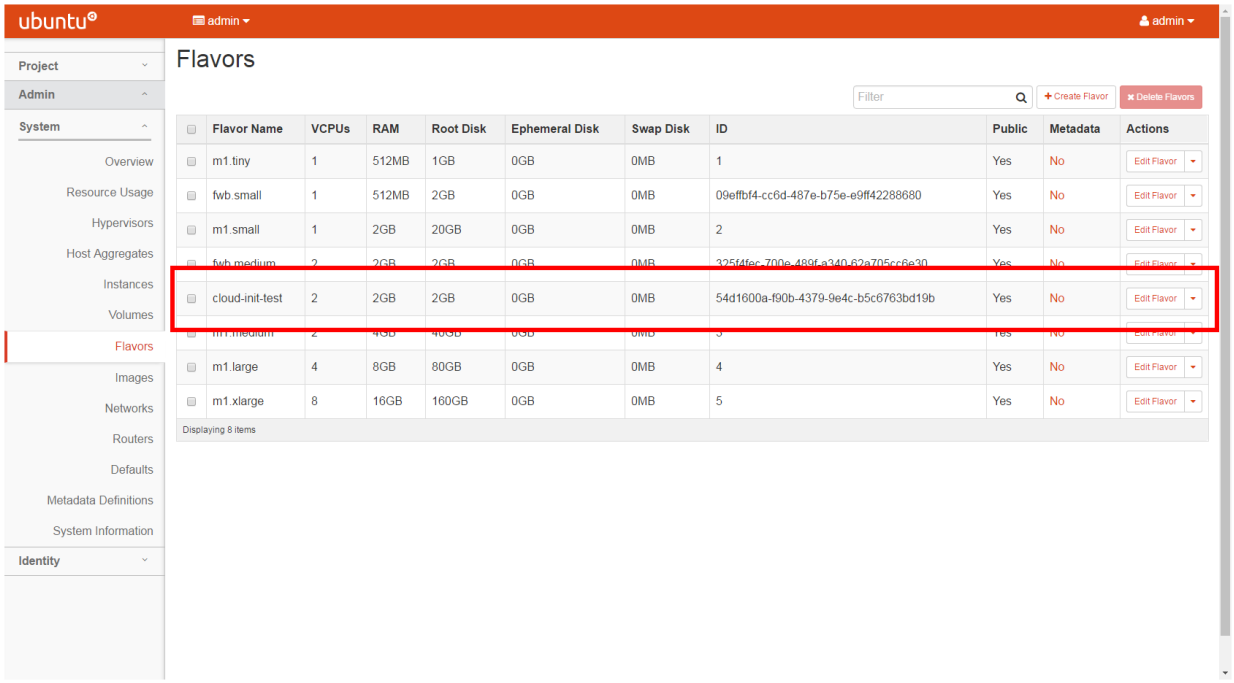
Alternatively, use the CLI command `nova volume-list` to verify the volume.

```
openstack@controller:~$
openstack@controller:~$ nova volume-list
WARNING: Command volume-list is deprecated and will be removed after Nova 13.0.0 is released. Use python-cinderclient or openstackclient instead.
+--------------------------------------+-----------+-------------------------+------+-------------+-------------+
| ID                                   | Status    | Display Name            | Size | Volume Type | Attached to |
+--------------------------------------+-----------+-------------------------+------+-------------+-------------+
| a4e7fe15-2d20-4090-adae-c85136fd87cf | available | cloud-init-test         | 30   | -           |             |
| be939e40-dbdd-4993-aeeb-f79a63204e63 | available | disk_src                | 30   |             |             |
| f87e5d5d-461c-473a-af05-81396c58d19d | available | lmydisk                 | 30   | -           |             |
| 6f6d921f-2826-48f6-a269-9927f36ceddc | available | voldisk1                | 30   | -           |             |
| 92b26eaa-dd4a-4d9d-9ce7-48efa0f7e1d5 | available | volum-551               | 30   | -           |             |
| c89c2db5-1aa8-4cf3-bb10-9aeaa9917a3e | available | yyy-ubuntu-server-14.04 | 20   | -           |             |
+--------------------------------------+-----------+-------------------------+------+-------------+-------------+
openstack@controller:~$
```

13. To specify the size of the instance, in the OpenStack dashboard, under **System**, navigate to the Flavors options and click **Create Flavor**.
14. Complete the flavor settings.



15. Click **Create Flavor**, and then use the dashboard to verify that OpenStack added the flavor.



16. Confirm the location of the initial FortiWeb configuration file you created earlier and the FortiWeb-VM license file.

See Preparing to deploy on OpenStack on page 131.

This example uploads the license as part of the boot process. Alternatively, you can omit the license file and upload it later. See Uploading the license on page 149.

```
openstack@controller:~$
openstack@controller:~$ cat lmy/user_data
config system global
  set hostname YZY-KVM-CLOUD-INIT
  set admintimeout 480
end
config system interface
  edit "port1"
    set type physical
    set allowaccess https ping ssh snmp http telnet
    set mode dhcp
    config  secondaryip
    end
  next
config system dns
  set primary 114.114.114.114
  set secondary 114.114.114.114
end

openstack@controller:~$ ls lmy/lic/FVVM080000059890.lic
lmy/lic/FVVM080000059890.lic
openstack@controller:~$
```

17. Use the following command to boot the instance:

```
nova boot --config-drive true --image <image_name> --flavor <flavor_name> --user-data
    <config_file> --file license=<fweb_license> --nic net-id=<network_id> --block-device-
    mapping vdb=<volume_id> <instance_name>
```

where:

`--config-drive true` enables OpenStack to write metadata to a special configuration drive that it attaches to the instance when it boots

`<image_name>` is the name of the FortiWeb-VM KVM image you uploaded earlier

`<flavor_name>` is the OpenStack flavor you configured earlier that specifies the size of the instance

`<config_file>` is the name and path of the initial configuration file you created earlier. It is the booting CLI configuration that FortiWeb uses. You can use this file for some public initialization configuration that scales the deployment.

`<fweb_license>` is the name and path of the FortiWeb license file

`<network_id>` is the ID of public network you created earlier for the instance to use

`<volume_id>` is the ID of the volume you created earlier to use as the FortiWeb log disk

`<instance_name>` is the name for the instance

For example (the image and the instance are both named cloud-init-test):

```
nova boot --config-drive true --image cloud-init-test --flavor 325f4fec-700e-489f-a340-
    62a705cc6e30 --user-data /home/openstack/lmy/user_data --file
    license=/home/openstack/lmy/lic/FVVM080000059890.lic --nic net-id=1146eb20-8828-45d3-
    a8a2-622276d344e4 --block-device-mapping vdb=a4e7fe15-2d20-4090-adae-c85136fd87cf
    cloud-init-test
```

18. OpenStack returns a table that allows you to confirm the instance configuration.

```
openstack@controller:~$
openstack@controller:~$ nova boot --config-drive true --image cloud-init-test --flavor 325f4fec-700e-489f-a340-62a705cc6e30 --user-data /home/openstack/lmy/user_data
 --file license=/home/openstack/lmy/lic/FVVM080000059890.lic --nic net-id=1146eb20-8828-45d3-a8a2-622276d344e4 --block-device-mapping vdb=a4e7fe15-2d20-4090-adae-c85
136fd87cf cloud-init-test
+--------------------------------------+------------------------------------------------------------+
| Property                             | Value                                                      |
+--------------------------------------+------------------------------------------------------------+
| OS-DCF:diskConfig                    | MANUAL                                                     |
| OS-EXT-AZ:availability_zone          |                                                            |
| OS-EXT-SRV-ATTR:host                 | -                                                          |
| OS-EXT-SRV-ATTR:hypervisor_hostname  | -                                                          |
| OS-EXT-SRV-ATTR:instance_name        | instance-0000015e                                          |
| OS-EXT-STS:power_state               | 0                                                          |
| OS-EXT-STS:task_state                | scheduling                                                 |
| OS-EXT-STS:vm_state                  | building                                                   |
| OS-SRV-USG:launched_at               | -                                                          |
| OS-SRV-USG:terminated_at             | -                                                          |
| accessIPv4                           |                                                            |
| accessIPv6                           |                                                            |
| adminPass                            | 3VcJp5YVggkU                                               |
| config_drive                         | True                                                       |
| created                              | 2016-05-09T08:01:29Z                                       |
| flavor                               | fwb.medium (325f4fec-700e-489f-a340-62a705cc6e30)          |
| hostId                               |                                                            |
| id                                   | 08e7ed2a-4d50-4346-8d9e-bb8064f6c7df                       |
| image                                | cloud-init-test (9c5f1433-0c64-4aa9-9461-d961a5eabe87)     |
| key_name                             | -                                                          |
| metadata                             | {}                                                         |
| name                                 | cloud-init-test                                            |
| os-extended-volumes:volumes_attached | [{"id": "a4e7fe15-2d20-4090-adae-c85136fd87cf"}]           |
| progress                             | 0                                                          |
| security_groups                      | default                                                    |
| status                               | BUILD                                                      |
| tenant_id                            | 483d1228407e4619a372705daf3f2f27                           |
| updated                              | 2016-05-09T08:01:31Z                                       |
| user_id                              | 19a68dc0448e410b9731ba79d8604422                           |
+--------------------------------------+------------------------------------------------------------+
openstack@controller:~$
```

19. Use the CLI command `nova list` to display the status of the instance and the IP address it was assigned.

```
openstack@controller:~$
openstack@controller:~$ nova list
+--------------------------------------+----------------+--------+------------+-------------+-------------------------------------------------------------------------------
--------------------+
| ID                                   | Name           | Status | Task State | Power State | Networks
                    |
+--------------------------------------+----------------+--------+------------+-------------+-------------------------------------------------------------------------------
--------------------+
| 08e7ed2a-4d50-4346-8d9e-bb8064f6c7df | cloud-init-test | ACTIVE | -          | Running     | public-network=10.200.71.175
                    |
| 723b7d5a-8e6a-46ad-b261-e0b1314096fd | cmic-test      | ACTIVE | -          | Running     | yzy-private-1=192.168.2.173, 10.200.71.167; yzy-2=192.168.5.101
                    |
| 5dba45ea-d810-42da-a295-56b848abfff3 | lmy-fwb-1      | ACTIVE | -          | Running     | lmy-private-2=192.168.11.105, 192.168.11.107; lmy-private-1=192.168.10
.114, 10.200.71.165 |
| a598131f-7bf0-4df3-aeb3-8d63c648c18b | yzy1           | ACTIVE | -          | Running     | public-network=10.200.71.137
                    |
+--------------------------------------+----------------+--------+------------+-------------+-------------------------------------------------------------------------------
--------------------+
openstack@controller:~$
```

20. Use Telnet or SSH to connect to the instance to confirm the initial configuration and that the license file has been uploaded to the FortiWeb.

```
openstack@controller:~$
openstack@controller:~$
openstack@controller:~$ telnet 10.200.71.175
Trying 10.200.71.175...
Connected to 10.200.71.175.
Escape character is '^]'.

YZY-KVM-CLOUD-INIT login: admin
Password:
Welcome!

YZY-KVM-CLOUD-IN~ # get system interface
== [ port1 ]
        type: physical
        ip: 10.200.71.175/16
        ip6: ::/0
        allowaccess: https ping ssh snmp http telnet
        status: up
        mode: dhcp
        description:
        ip6-allowaccess:
        wccp: disable
        mtu: 1500

YZY-KVM-CLOUD-IN~ # get system dns
primary             : 114.114.114.114
secondary           : 114.114.114.114
domain              :

YZY-KVM-CLOUD-IN~ # get system status
International version: FortiWeb-KVM 5.55,build0751,180504
Serial-Number: FVVM080000059890
BIOS version: 04000002
Log hard disk: Available
Hostname: YZY-KVM-CLOUD-INIT
Operation Mode: Reverse Proxy
FIPS-CC mode: disabled
Current HA mode: standalone

YZY-KVM-CLOUD-IN~ #
```

21. Continue with the appliance configuration using the CLI or access the web UI using the assigned IP address (example, using `https://10.200.71.175`). For complete configuration information, see the *FortiWeb Administration Guide*.

Configuring access to FortiWeb's web UI & CLI

For hypervisor deployments, after the virtual appliance is powered on, you log in to the FortiWeb-VM command line interface (CLI) via the console and configure basic network settings so that you can connect to the appliance's web UI, CLI, or both through your management computer's network connection.

For FortiWeb-VM deployed on AWS, you access the web UI using the public DNS address displayed in the instance information for the appliance in your AWS console or an SSH connection. For instructions, see Deploying FortiWeb-VM on AWS EC2 on page 19.

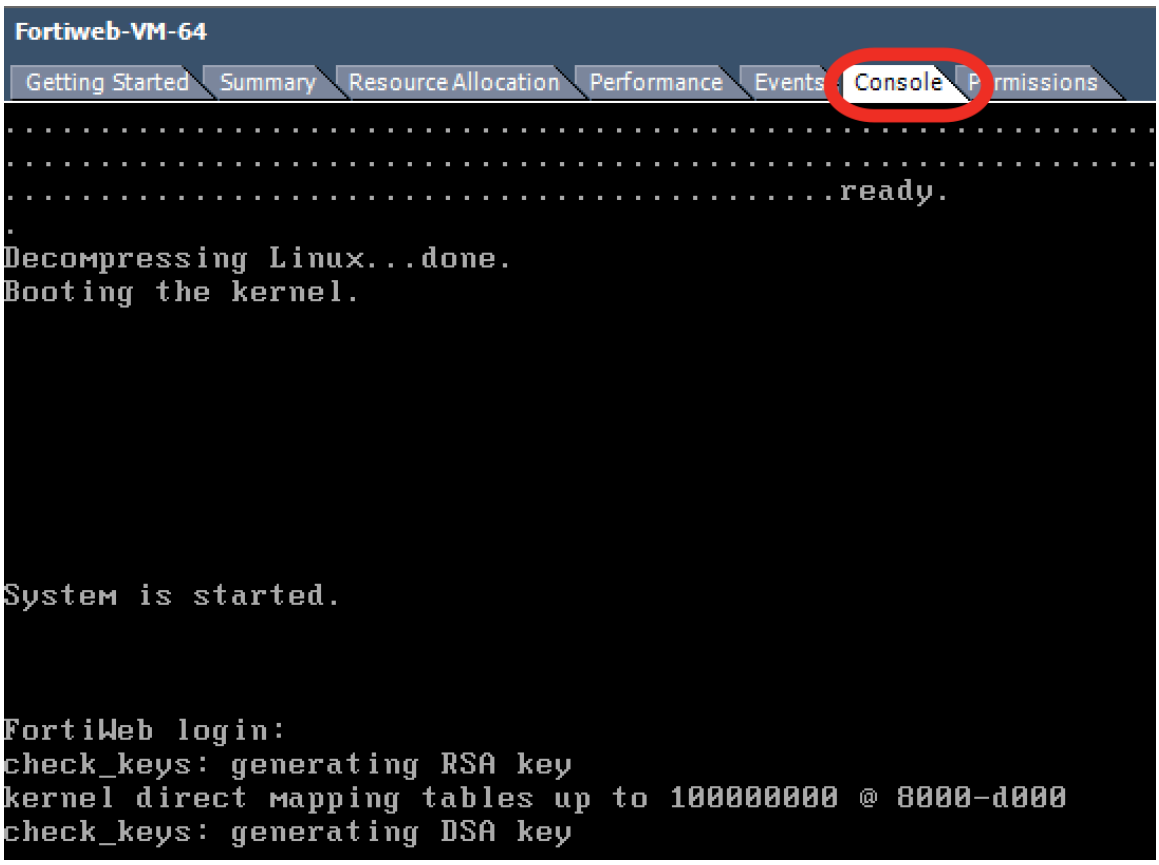
To configure basic network settings for FortiWeb-VM deployed on a hypervisor

1. On your management computer, start one of the following, depending on the VM environment in which you have deployed FortiWeb-VM:
   - VMware vSphere Client
   - Citrix XenCenter
   - Xen Project Virtual Machine Manager (`virt-manager`) or a VNC viewer
   - Hyper-V Manager
2. Log in to the VM server.
3. Open the console of the FortiWeb-VM virtual appliance.

   On VMware vSphere Client:

   - In the pane on the left side, select the name of the virtual appliance, such as **FortiWeb-VM**.
   - Click the **Console** tab.

Console tab in VMware vSphere Client



On Citrix XenCenter:

- In the pane on the left side, select the name of the virtual appliance, such as **FortiWeb-VM**.

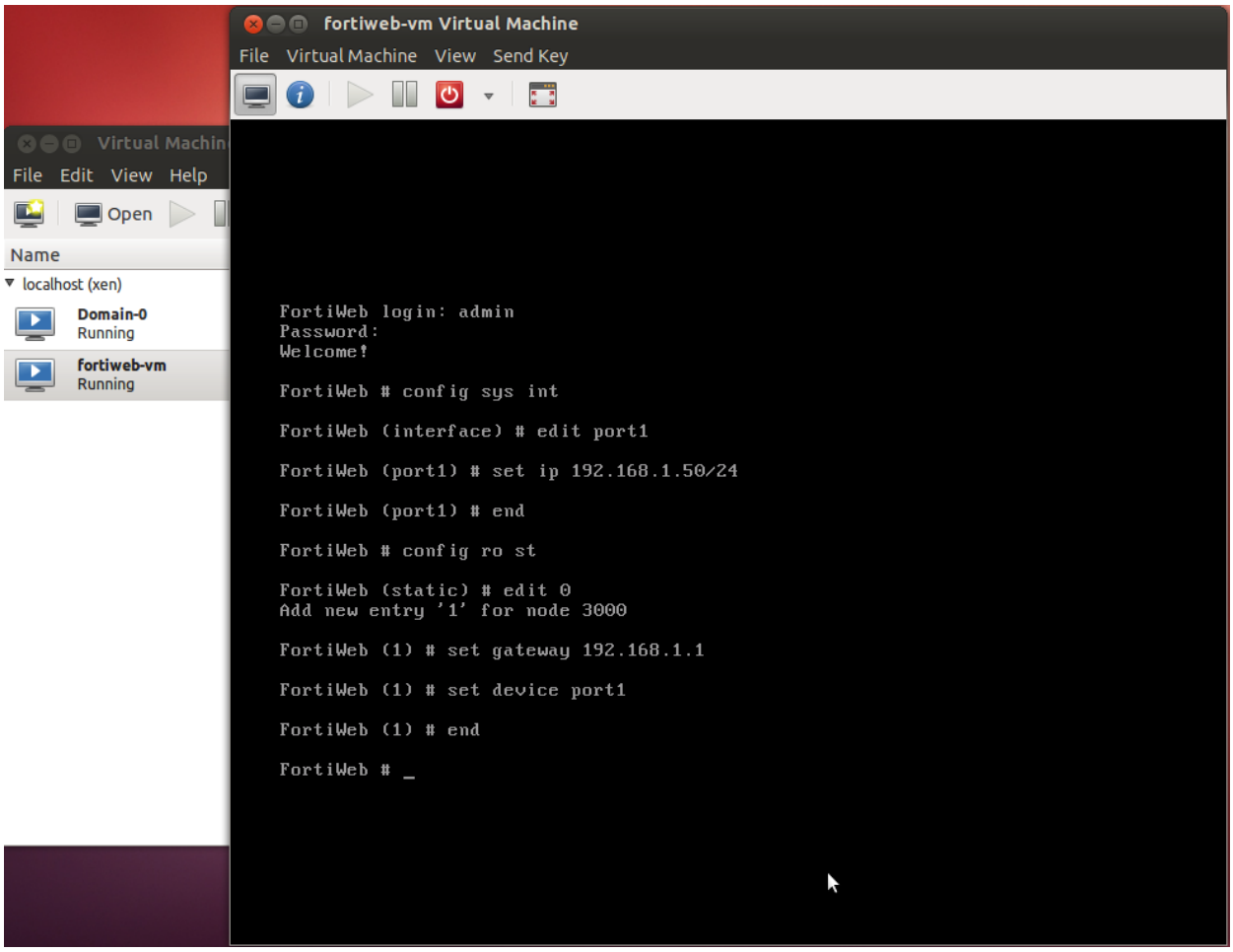
  Several tabs for that virtual machine will appear in the pane on the right side.

- Click the **Console** tab.

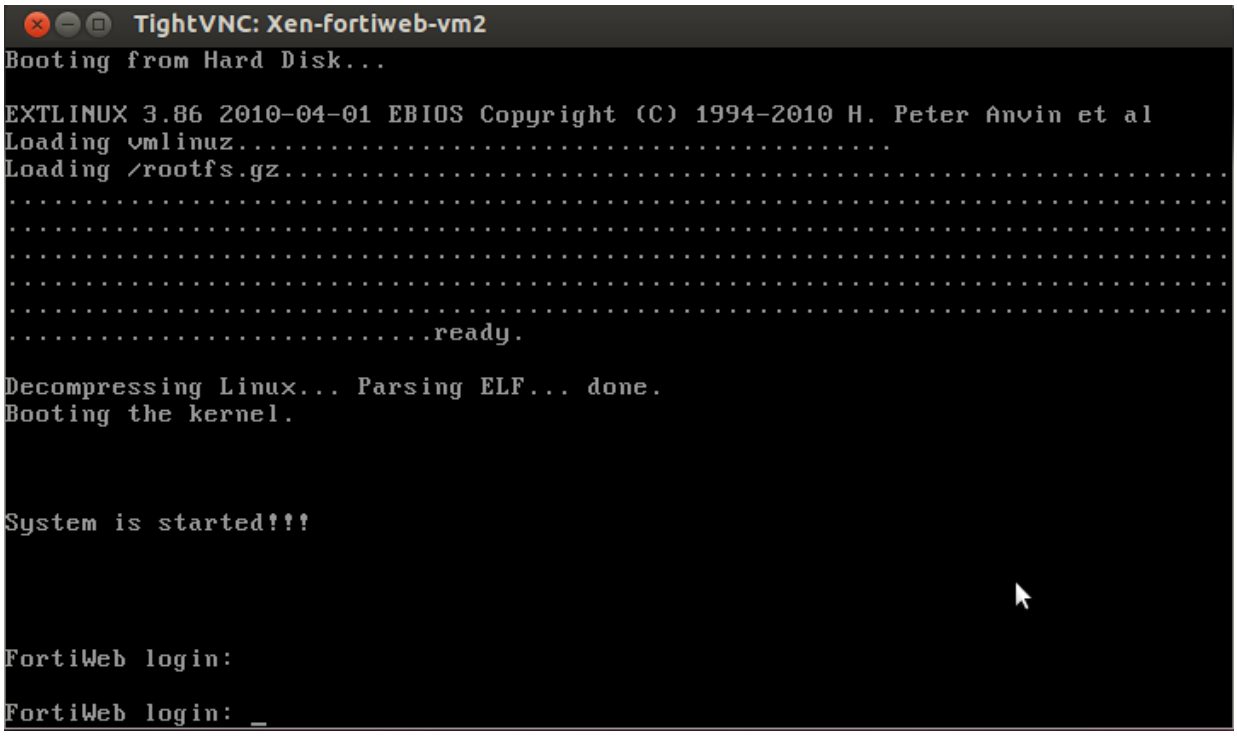
On Virtual Machine Manager:

- In the pane on the left side, select the name of the virtual appliance, such as **FortiWeb-VM**.
- Click **Open**.

- In the window that appears, click the monitor icon.



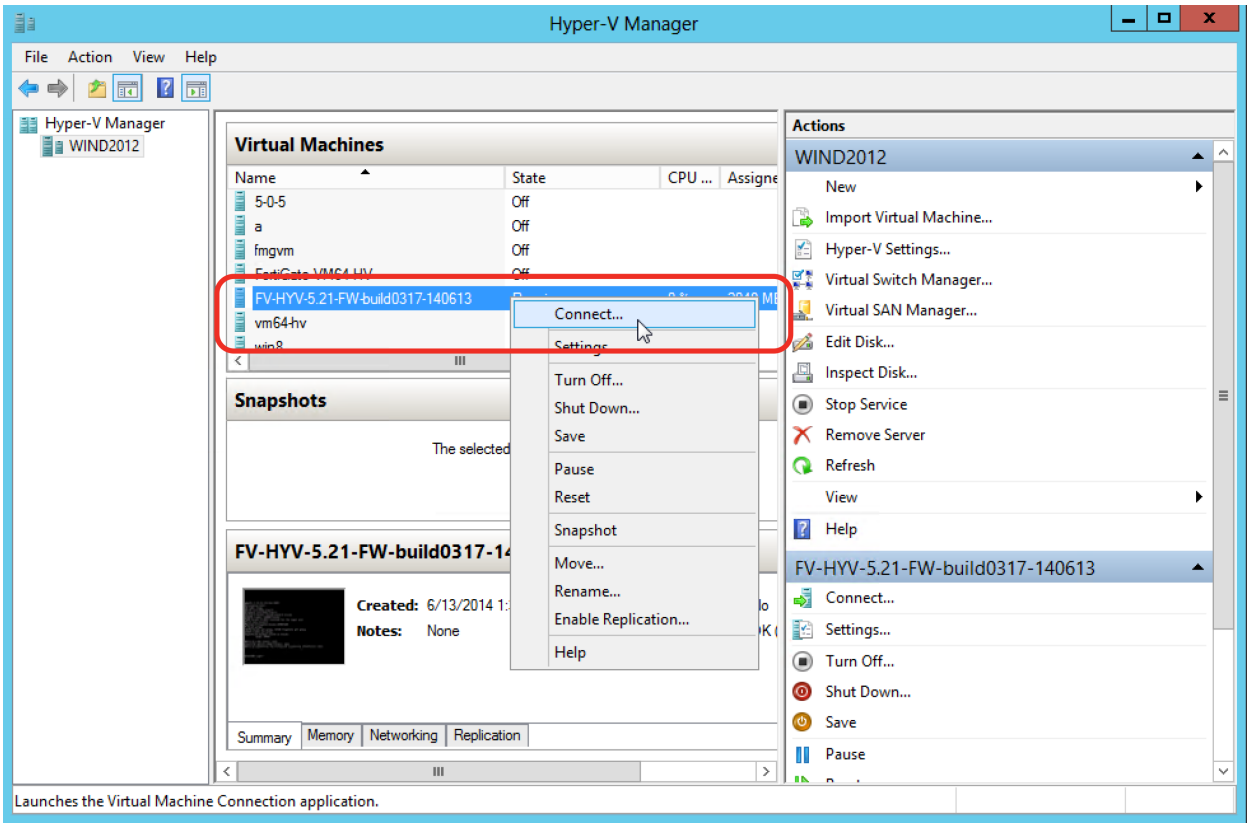
On a VNC client, connect to the IP address of the Xen Project server and the port number allocated to that instance of FortiWeb-VM.



On Hyper-V Manager:

- Under **Virtual Machines**, right-click the name of the virtual appliance, such as **FortiWeb-VM**.

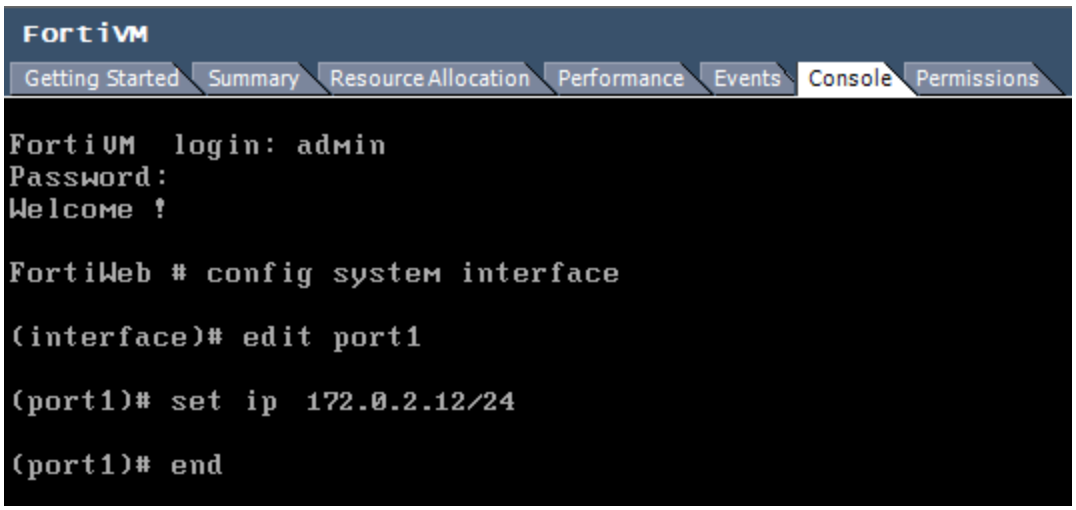
- Click **Connect**.



4. At the login prompt for the local console, type:

   `admin`

5. Press Enter twice. (Initially, there is no password.)



6. Configure the IP address and netmask of the network interface named `port1`, or whichever network interface maps to the network physically connected to your management computer. Type:

```
config system interface
edit port1
set ip <address_ip> <netmask_ip>
end
```

where:

- `<address_ip>` is the IPv4 or IPv6 address assigned to the network interface, such as `192.168.1.99`; the correct IP will vary by your configuration of the vNetwork (see Mapping the virtual NICs (vNICs) to physical NICs on page 36)
- `<netmask_ip>` is its netmask in dotted decimal format, such as `255.255.255.0` (alternatively, append a CIDR-style subnet such as /24 to the IP)

7. Configure the primary and secondary DNS server IP addresses. Type:

```
config system dns
set primary <dns_ip>
set secondary <dns_ip>
end
```

where `<dns_ip>` is the IPv4 or IPv6 address of a DNS server.

8. Configure a static route with the default gateway. Type:

```
config router static
edit 0
set gateway <router_ip>
set device port1
end
```

where `<router_ip>` is the IP address of the gateway router.

You should now be able to connect via the network from your management computer to `port1` of FortiWeb-VM using:

- a web browser for the web UI (e.g. If `port1` has the IP address 192.168.1.1, go to https://192.168.1.1/)
- an SSH client for the CLI (e.g. If `port1` has the IP address 192.168.1.1, connect to 192.168.1.1 on port 22.)

When connecting to the web UI via HTTPS, if you cannot get a connection, verify that your computer's time zone matches the appliance's configured system time. For more first-time connection troubleshooting, or instructions on how to configure the time and time zone, see the *FortiWeb Administration Guide*.

9. Continue by uploading the license file. (See Uploading the license on page 149. For the FortiWeb Manager license, see the *FortiWeb Manager Handbook*.)

If you are using the 15-day free trial license and do not yet have a paid license file, you can continue instead with What's next? on page 157.

When the 15-day free trial license expires, you will not be able to perform any actions in the web UI until a license has been uploaded. After a valid license has been uploaded, the web UI and the CLI will be unlocked and fully functional.

The trial period begins the first time you power on your FortiWeb-VM virtual appliance. You can upgrade the trial license to a purchased one at any time during or after the trial period by uploading the license file via the **License Information** widget in the dashboard of the web UI. For instructions, see Uploading the license on page 149.

Uploading the license

When you purchase a license for FortiWeb-VM, Fortinet Technical Support (https://support.fortinet.com) provides a license file that you can use to convert the 15-day trial license to a permanent, paid license.

(Licensing for FortiWeb Manager virtual machine is different. See the *FortiWeb Manager Handbook*.)

You can upload the license via a web browser connection to the web UI or the CLI. No maintenance period scheduling is required. The uploading process does not interrupt traffic or trigger an appliance reboot.

As your organization grows, you can simply either allocate more resources or migrate your virtual appliance to a physical server with more power, then upgrade your FortiWeb-VM license to support your needs.

License validation without Internet connectivity (closed network)

FortiWeb-VM requires an Internet connection to periodically re-validate its license. If FortiWeb-VM cannot contact Fortinet's FDN for 24 hours, access to the web UI and CLI are locked.

Alternatively, in a closed network environment, you can validate your FortiWeb-VM license using FortiManager's built-in FDS (FortiGuard Distribution Servers) feature. To configure FortiWeb-VM to validate its license using FortiManager, before you upload the license, enter the following command:

```
config system autoupdate override
   set status enable
   set address <fortimanager_ip>:8890
   set fail-over disable
end
```

where `<fortimanager_ip>` is the IP address of the FortiManager. (TCP port 8890 is the port where the built-in FDS feature listens for requests.)

For more information on the FortiManager built-in FDB feature, see the *FortiManager Administration Guide*.

Although FortiManager can provide FortiGuard security service updates to some Fortinet devices, for FortiWeb, its FDN features can provide license validation only.

To upload the license via the web UI

1. On your management computer, start a web browser.

   For hypervisor installations, your computer must be connected to the same network as the hypervisor.

2. Do one of the following:

   - For hypervisor deployments, in your browser's URL or location field, enter the IP address of `port1` of the virtual appliance, such as:

     https://192.168.1.99/

     (Remember to include the "s" in https://.)

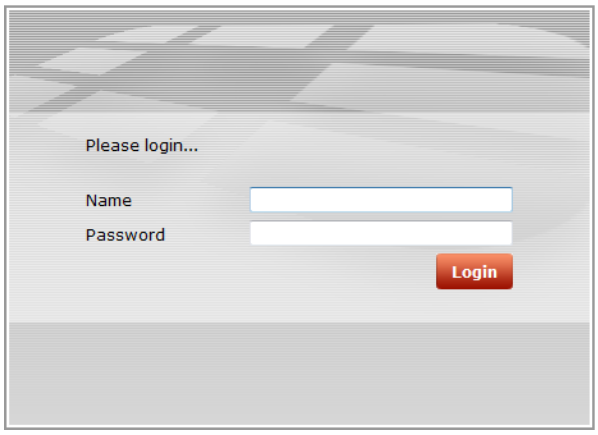
Initially, you must access the web UI via HTTPS. By default, HTTP is not enabled. After uploading the license, you can configure the administrative access protocols. For details, see the *FortiWeb Administration Guide*.

- For FortiWeb-VM deployed on AWS, access the web UI using the public DNS address displayed in the instance information for the appliance in your AWS console.

  For example, if the public DNS address is `ec2-54-234-142-136.compute-1.amazonaws.com`, you connect to the web UI using the following URL:

  `https://ec2-54-234-142-136.compute-1.amazonaws.com/`

Your browser connects the appliance. The web UI's login page should appear.



If you do **not** see the login page due to an SSL cipher error during the connection, and you are connecting to the trial license of FortiWeb-VM or a LENC version of FortiWeb, then your browser must be configured to accept encryption of 64-bit strength or less during the handshake. (RC2, RC4, and DES with less than 64-bit strength is supported. AES and 3DES is **not** supported in these versions.) Otherwise SSL v3 and TLS v1.0 are supported.

For example, in Mozilla Firefox, if you receive this error message:

`ssl_error_no_cypher_overlap`

you may need to enter `about:config` in the URL bar, then set **security.ssl3.rsa.rc4_40_md5** to **true**.

To support HTTPS authentication, the FortiWeb appliance ships with a self-signed X.509 certificate, which it presents to clients whenever they initiate an HTTPS connection to the FortiWeb appliance. When you connect, depending on your web browser and prior access of the FortiWeb appliance, your browser might display two security warnings related to this certificate:

- The certificate is not automatically trusted because it is self-signed, rather than being signed by a valid certificate authority (CA). Self-signed certificates cannot be verified with a proper CA, and therefore might be fraudulent. You must manually indicate whether or not to trust the certificate.
- The certificate might belong to another web site. The common name (CN) field in the certificate, which usually contains the host name of the web site, does not exactly match the URL you requested. This could indicate server identity theft, but could also simply indicate that the certificate contains a domain name while you have entered an IP address. You must manually indicate whether this mismatch is normal or not.

Both warnings are normal for the default certificate.

3. Verify and accept the certificate, either permanently (the web browser will not display the self-signing warning again) or temporarily. You cannot log in until you accept the certificate.
4. For details on accepting the certificate, see the documentation for your web browser.
5. In the *Name* field, type `admin`.

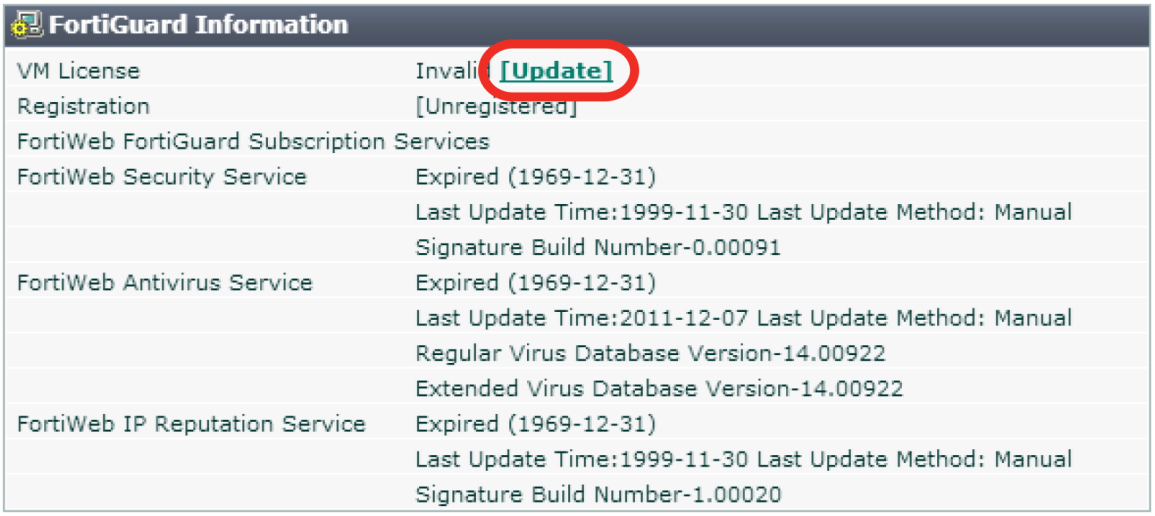
   Do one of the following:

   - For hypervisor deployments, do not enter a password.
   - For AWS deployments, for **Password**, enter the AWS instance ID.
6. Click **Login**.

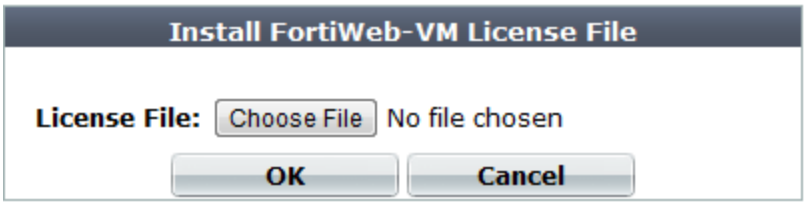
   The web UI appears.

   The web UI initially displays its dashboard, **System > Status > Status**. The **FortiGuard Information** widget displays the current license status and contains a link where you can upload a license file.

FortiGuard Information widget on System > Status > Status in the web UI before license upload



7. In the **VM License** row of the **FortiGuard Information** widget, click the **Update** link.



8. Depending on your browser, you may see either a **Browse** or **Choose File** button. Locate the license file (.lic) you downloaded earlier from Fortinet, then click **OK**.

   Your browser uploads the license file. Time required varies by the size of the file and the speed of the network connection. If you have uploaded a file that is not a license file, an error message will appear:

   ```
   Uploaded file is not a license. Please upload a valid license.
   ```

If you upload the right file type, FortiWeb will then connect to Fortinet to validate its license. Time required varies, but is usually only a few seconds. A message appears:

```
License has been uploaded. Please wait for authentication with registration
    servers.
```

9. Click **Refresh** on the message box.

   If you uploaded a valid license, a second message should appear, informing you that your license authenticated successfully:

   ```
   License has been successfully authenticated with registration servers.
   ```

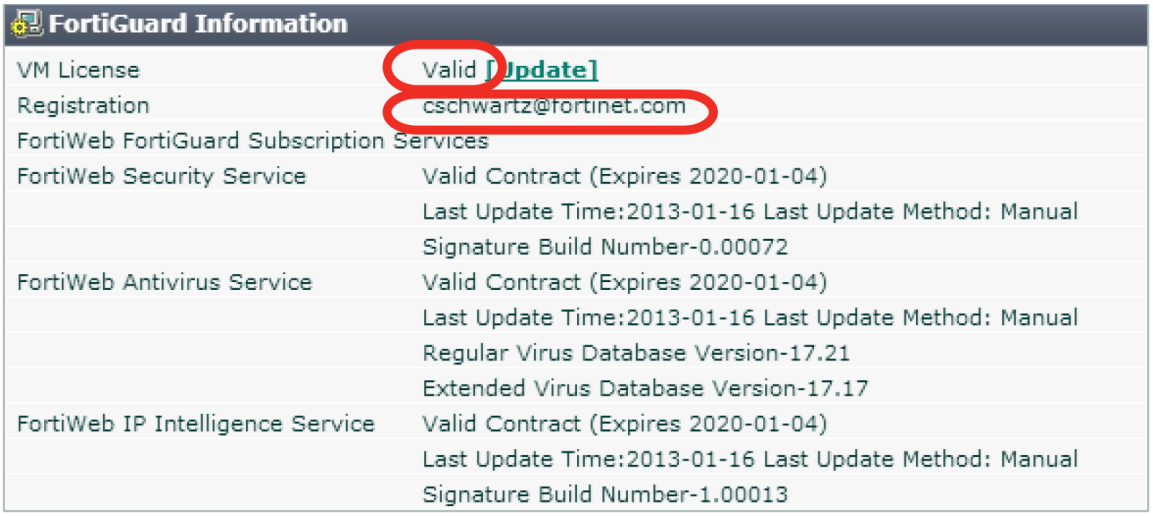
   The web UI logs you out. The login dialog reappears.

10. Log in again.

11. To verify that the license was uploaded successfully, log in to the web UI again, then view the **FortiGuard Information** widget. The **VM License** row should say **Valid**.

    Also view the **System Information** widget. The **Serial Number** row should have a number that indicates the maximum number of vCPUs that can be allocated according to the FortiWeb-VM software license, such as **FVVM020000003619** (where "VM02" indicates a limit of 2 vCPUs).

FortiGuard Information widget on System > Status > Status in the web UI after license validation



GUI item	Description
VM License	Indicates whether or not this FortiWeb-VM appliance has a paid software license. The license affects the maximum number of allocatable vCPUs. Possible states are: • **Valid** — The appliance has a valid, non-trial license. **Serial Number** in the **System Information** widget indicates the maximum number of vCPUs that can be allocated according to this license. To increase the number of vCPUs that this appliance can utilize, invalidate the current license by allocating more vCPUs in your virtual machine environment (e.g. VMware), then upload a new license. See Updating the license for more vCPUs on page 155. • **Invalid** — The FortiWeb-VM appliance license either was **not** valid, **or** is currently a **trial** license. To upload a purchased license, click **Update**. This appears only in FortiWeb-VM.
Registration	Indicates which account registered this appliance with Fortinet Technical Support. Possible states are: • **Unregistered** — Not registered with Fortinet Technical Support. • **<registration_email>** — Registered with Fortinet Technical Support. To manage technical support or FortiGuard service contracts for this device, go to the Fortinet Technical Support web site.

If logging is enabled, this log message will be recorded in the event log:

```
License status changed to VALID
```

If you are still connected to the CLI when license authentication succeeds, it should print this message:

```
*ATTENTION*: license registration status changed to 'VALID',please logout and re-login
```

If FortiWeb was also able to contact FortiGuard, its **FortiWeb Update Service** row should also indicate that the FortiGuard service contract is valid. (This second license validation may occur a minute or two after the first, and so may not appear immediately.)

If there was a connectivity interruption, you can either wait up to 30 minutes for the next license query, reboot, or enter the CLI command:

```
exec update-now
```

This command also contacts FortiGuard for FortiWeb Security Service contract validation and update availability.

If the connection did **not** succeed:

- On FortiWeb, verify the:
  - time zone & time
  - DNS settings
  - network interface up/down status & IP
  - static routes
- On your computer, use `nslookup` to verify that FortiGuard domain names are resolving (VM license queries are sent to `update.fortiguard.net`).

```
C:\Users\cschwartz>nslookup update.fortiguard.net
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: fds1.fortinet.com
Addresses: 209.66.81.150
209.66.81.151
208.91.112.66
Aliases: update.fortiguard.net
```

- On FortiWeb, use `execute ping` and `execute traceroute` to verify that connectivity from FortiWeb to the Internet and FortiGuard is possible. Check the configuration of any NAT or firewall devices that exist between the FortiWeb appliance and the FDN or FDS server override.

```
FortiWeb # exec traceroute update.fortiguard.net
traceroute to update.fortiguard.net (209.66.81.150), 32 hops max, 84 byte packets
1 192.0.2.2 0 ms 0 ms 0 ms
2 209.87.254.221 <static-209-87-254-221.storm.ca> 4 ms 2 ms 3 ms
3 209.87.239.161 <core-2-g0-3.storm.ca> 2 ms 3 ms 3 ms
4 67.69.228.161 3 ms 4 ms 3 ms
5 64.230.164.17 <core2-ottawa23_POS13-1-0.net.bell.ca> 3 ms 5 ms 3 ms
6 64.230.99.250 <tcore4-ottawa23_0-4-2-0.net.bell.ca> 16 ms 17 ms 15 ms
7 64.230.79.222 <tcore3-montreal01_pos0-14-0-0.net.bell.ca> 14 ms 14 ms 15 ms
8 64.230.187.238 <newcore2-newyork83_so6-0-0_0> 63 ms 15 ms 14 ms
9 64.230.187.42 <bxX5-newyork83_POS9-0-0.net.bell.ca> 21 ms 64.230.187.93 <BX5-
    NEWYORK83_POS12-0-0_core.net.bell.ca> 17 ms 16 ms
10 67.69.246.78 <Abovenet_NY.net.bell.ca> 28 ms 28 ms 28 ms
11 64.125.21.86 <xe-1-3-0.cr2.lga5.us.above.net> 29 ms 29 ms 30 ms
12 64.125.27.33 <xe-0-2-0.cr2.ord2.us.above.net> 31 ms 31 ms 33 ms
13 64.125.25.6 <xe-4-1-0.cr2.sjc2.us.above.net> 82 ms 82 ms 100 ms
14 64.125.26.202 <xe-1-1-0.er2.sjc2.us.above.net> 80 ms 79 ms 82 ms
15 209.66.64.93 <209.66.64.93.t01015-01.above.net> 80 ms 80 ms 79 ms
16 209.66.81.150 <209.66.81.150.available.above.net> 83 ms 82 ms 81 ms
```

If after 4 hours FortiWeb still cannot validate its license, a warning message will be printed to the local console:

```
*WARNING*: Unable to validate license for over 4 hours
```

12. Continue with What's next?.

To upload the license via the CLI

1. Using an SSH client, log in to the CLI using the IP address of the network interface you configured earlier.

For example, if you configured `port1` with the IP address `192.168.1.1`, connect to `192.168.1.1` on port 22.

For more information, see Configuring access to FortiWeb's web UI & CLI on page 143.

2. Enter the following command:

```
execute restore vmlicense {ftp | tftp} <license-file_str> {<ftp_ipv4> | <user_
    str>:<password_str>@<ftp_ipv4> | <tftp_ipv4>}
```

where:

`{ftp | tftp}` specifies whether to connect to the server using file transfer protocol (FTP) or trivial file transfer protocol (TFTP).

`<license-file_str>` is the name of the license file.

`{<ftp_ipv4>` is the IP address of the FTP server.

`<user_str>` is the user name that FortiWeb uses to authenticate with the server.

`<password_str>` is the password for the account specified by `<user_str>`.

`<tftp_ipv4>` is the IP address of the TFTP server.

3. Confirm that you want to perform the license upload.

After the license is authenticated successfully, the following message is displayed:

```
"*ATTENTION*: license registration status changed to 'VALID', please logout and re-
    login"
```

For information on troubleshooting a license upload, see To upload the license via the web UI on page 149.

4. Continue with What's next?.

Updating the license for more vCPUs

If either:

- you want to upgrade FortiWeb-VM to a license with a higher vCPU limit
- your original FortiWeb-VM license was an extended (but temporary) evaluation license, and you have now purchased a permanent, paid license

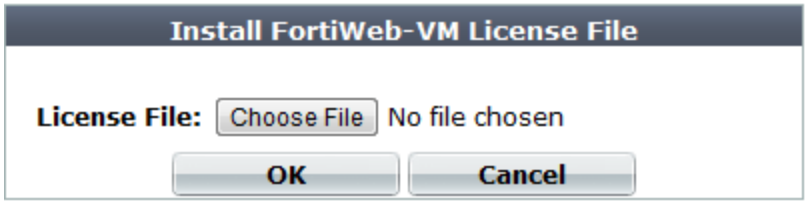
you must upload a new license file.

To replace an evaluation license with a paid license, use Uploading the license on page 149.

To allocate more vCPUs

1. Log in to FortiWeb-VM as `admin` via the web UI.
2. Go to **System > Status > Dashboard**.

3. Upload the new license. For details, see Uploading the license on page 149.



4. In the **System Information** widget, click **Shut Down**.

   The virtual appliance will flush its data to its virtual disk, and prepare to be powered off. If you skip this step and immediately power off FortiWeb-VM, you may lose buffered data.

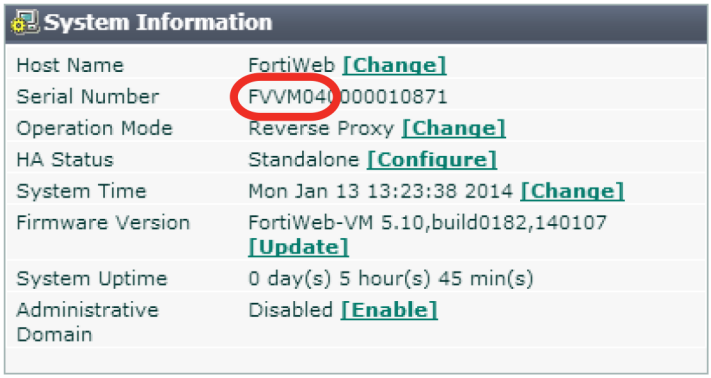
5. On your management computer, start your central management client, connect and log in to the server that is currently hosting FortiWeb-VM.
6. In the pane on the left side, click the name of the virtual appliance, such as **FortiWeb-VM**.
7. Power off the virtual machine.
8. Increase the vCPU allocation. For details, see one of the following topics:

   - Configuring the number of virtual CPUs (vCPUs) on page 32 (VMware vSphere)
   - Configuring the number of virtual CPUs (vCPUs) on page 70 (Citrix Xen)
   - Deploying via Virtual Machine Manager on page 92 (Xen Project)
   - Configuring the number of virtual CPUs (vCPUs) on page 115 (Hyper-V)

9. Power on the virtual appliance again.

   FortiWeb-VM evaluates its current license and discovers that you have allocated an unsupported number of vCPUs, causing the current license to become invalid.

10. Log in to the web UI again. In the **License Information** widget, the maximum number of vCPUs allowed by your FortiWeb-VM license should now match the VMware setting.



What's next?

At this point, the FortiWeb-VM virtual appliance is running, and it has received a license file, but its operating system is almost entirely unconfigured. Before you can use FortiWeb-VM, you must configure it.

Configure the FortiWeb-VM software using the *FortiWeb Administration Guide*.

After you have completed this first-time setup, you can refer to the *FortiWeb Administration Guide* and/or *FortiWeb CLI Reference*. Updates, reconfiguration, and ongoing use of both FortiWeb-VM virtual appliances and physical appliance models such as FortiWeb-3000C are the same.

Updating the virtual hardware

By default, FortiWeb-VM uses VMware virtual hardware version 5. If you need to update your FortiWeb-VM's virtual hardware, shut down FortiWeb-VM before doing so.

For example, if you have a VMware vSphere ESXi 5.1 environment that supports virtual hardware version 9, and you want to provide version 9 feature support such as backups to FortiWeb-VM, you would update the virtual hardware.

For more information on virtual hardware, see:

http://kb.vmware.com/selfservice/documentLinkInt.do?micrositeID=&popup=true&languageId=&externalID=1010675

To update the virtual hardware

1. Shut down FortiWeb-VM. To do this, you can enter the CLI command:

   ```
   execute shutdown
   ```

2. In VMware vCenter, right-click the VM and select the option to upgrade the virtual hardware.
3. When the upgrade is complete, power on FortiWeb-VM.